

IBM Spectrum Protect Knowledge Center Version 8.1.3



Tabla de contenido

Bienvenido	1
Accesibilidad	1
Suites de producto y productos relacionados	2
Archivos PDF	4
Actualizaciones en este release	4
Conceptos de IBM Spectrum Protect	5
Visión general de IBM Spectrum Protect	5
Componentes de protección de datos	5
Servicios de protección de datos	6
Procesos de gestión de protección de datos	8
Interfaces de usuario	11
Conceptos de almacenamiento de datos	11
Dispositivos de almacenamiento de datos	12
Agrupaciones de almacenamiento	15
Transporte de datos a almacenar	19
Estrategias de protección de datos	22
Minimización del espacio de almacenamiento de copias de seguridad	22
Estrategias de protección ante desastres	23
Conceptos de la recuperación tras desastre	27
Soluciones de protección de datos	28
Selección de una solución de protección de datos	28
Solución de disco de sitio único	29
Solución de disco multisitio	30
Solución de dispositivo multisitio	30
Solución de cinta	31
Comparación de soluciones	32
Hoja de ruta de la solución	34
Solución de disco de sitio único	34
Planificación	35
Selección de un tamaño del sistema	36
Requisitos del sistema para una solución de disco de sitio único	37
Requisitos de hardware	37
Requisitos de software	38
Planificación de hojas de trabajo	39
Planificación de almacenamiento	49
Planificación de la seguridad	50
Planificación de los roles de administración	50
Planificación para comunicaciones seguras	51
Planificación de almacenamiento de datos cifrados	51
Planificación del acceso de cortafuegos	51
Implementación	52
Configuración del sistema	53
Configuración del hardware de almacenamiento	53
Instalación del sistema operativo del servidor	53
Instalación en sistemas AIX	54
Instalación en sistemas Linux	55

Instalación en sistemas Windows	59
Configuración de E/S de la multivía de acceso	59
Sistemas AIX	59
Sistemas Linux	60
Sistemas Windows	61
Creación del ID de usuario para el servidor	62
Preparación de sistemas de archivos para el servidor	63
Sistemas AIX	63
Sistemas Linux	64
sistemas Windows	65
Instalación del servidor y Centro de operaciones	65
Instalación en sistemas AIX y Linux	65
Instalación en sistemas Windows	66
Configuración del servidor y el Centro de operaciones	67
Configuración de la instancia de servidor	67
Instalación del cliente de archivado y copia de seguridad	68
Configuración de opciones para el servidor	69
Configuración de comunicaciones seguras con Seguridad de la capa de transporte	70
Configuración de Centro de operaciones	70
Registro de la licencia de producto	71
Configuración de la optimización de almacenamiento de datos	71
Definición de las reglas de retención de datos para su empresa	72
Definición de planificaciones para actividades de mantenimiento del servidor	72
Definición de planificaciones de cliente	74
Instalación y configuración de clientes de archivado y copia de seguridad	74
Registro y asignación de clientes a planificaciones	75
Instalación del servicio de gestión de cliente	75
Verificación de que el servicio de gestión de clientes está instalado correctamente	76
Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente	77
Finalización de la implementación	78
Supervisión	78
Lista de comprobación diaria	78
Lista de comprobación periódica	85
Verificación de la conformidad de licencia	91
Seguimiento del estado del sistema mediante informes de correo electrónico	92
Gestión	93
Gestión del Centro de operaciones	94
Adición y eliminación de servidores spoke	94
Adición de un servidor de radio	94
Eliminación de un servidor spoke	95
Inicio y detención del servidor web	95
Reinicio del asistente de configuración inicial	96
Cambio del servidor concentrador	97
Restauración de la configuración a un estado de preconfiguración	97
Protección de aplicaciones, máquinas virtuales y sistemas	98
Adición de clientes	98
Selección del software de cliente y planificación de la instalación	99
Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	101
Visualización de políticas	101
Edición de políticas	102
Planificación de copia de seguridad y operaciones de archivado	103
Registro de clientes	104
Instalación y configuración de clientes	104
Configuración del cliente para ejecutar las operaciones planificadas	106
Configuración de comunicaciones a través de un cortafuegos	107
Gestión de operaciones de cliente	108
Evaluación de errores en registros de errores de cliente	108
Detención y reinicio del aceptador de cliente	109

Restablecimiento de contraseñas	110
Modificación del ámbito de una copia de seguridad de cliente	111
Gestión de actualizaciones del cliente	111
Poner fuera de servicio un nodo cliente	112
Desactivación de datos para liberar espacio de almacenamiento	114
Gestión del almacenamiento de datos	114
Auditoría de un contenedor de la agrupación de almacenamiento	114
Gestión de la capacidad de inventario	115
Gestión del uso de la memoria y del procesador	117
Ajuste de actividades planificadas	117
Protección del servidor	118
Conceptos sobre la seguridad	118
Gestión de administradores	120
Cambio de los requisitos de contraseña	120
Protección del servidor en el sistema	121
Restricción del acceso de usuario al servidor	122
Limitación de acceso a través de restricciones de puerto	122
Detención e inicio del servidor	123
Detención del servidor	123
Inicio del servidor para tareas de mantenimiento o reconfiguración	124
Planificación para actualizar el servidor	125
Preparación para una parada	125
Implementación de un plan de recuperación tras desastre	126
Recuperación de paradas del sistema	126
Solución de disco multisitio	127
Planificación	127
Selección de un tamaño del sistema	128
Planificación de los sitios	129
Requisitos del sistema para una solución de disco multisitio	130
Requisitos de hardware	130
Requisitos de software	132
Planificación de hojas de trabajo	133
Planificación de almacenamiento	142
Planificación de la seguridad	143
Planificación de los roles de administración	143
Planificación para comunicaciones seguras	144
Planificación de almacenamiento de datos cifrados	144
Planificación del acceso de cortafuegos	144
Implementación	146
Configuración del sistema	146
Configuración del hardware de almacenamiento	147
Instalación del sistema operativo del servidor	147
Instalación en sistemas AIX	147
Instalación en sistemas Linux	149
Instalación en sistemas Windows	152
Configuración de E/S de la multivía de acceso	153
Sistemas AIX	153
Sistemas Linux	154
Sistemas Windows	155
Creación del ID de usuario para el servidor	155
Preparación de sistemas de archivos para el servidor	156
Sistemas AIX	156
Sistemas Linux	157
sistemas Windows	158
Instalación del servidor y Centro de operaciones	159
Instalación en sistemas AIX y Linux	159
Instalación en sistemas Windows	160
Configuración del servidor y el Centro de operaciones	160

Configuración de la instancia de servidor	161
Instalación del cliente de archivado y copia de seguridad	162
Configuración de opciones para el servidor	162
Configuración de comunicaciones seguras con Seguridad de la capa de transporte	163
Configuración de Centro de operaciones	163
Registro de la licencia de producto	164
Configuración de la optimización de almacenamiento de datos	165
Definición de las reglas de retención de datos para su empresa	165
Definición de planificaciones para actividades de mantenimiento del servidor	166
Definición de planificaciones de cliente	168
Instalación y configuración de clientes de archivado y copia de seguridad	168
Registro y asignación de clientes a planificaciones	168
Instalación del servicio de gestión de cliente	169
Verificación de que el servicio de gestión de clientes está instalado correctamente	169
Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente	170
Configuración del segundo servidor	171
Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke	171
Añadir un segundo servidor como servidor spoke	173
Habilitación de réplica	173
Finalización de la implementación	173
Supervisión	174
Lista de comprobación diaria	174
Lista de comprobación periódica	181
Verificación de la conformidad de licencia	187
Seguimiento del estado del sistema mediante informes de correo electrónico	188
Gestión	189
Gestión del Centro de operaciones	190
Adición y eliminación de servidores spoke	190
Adición de un servidor de radio	190
Eliminación de un servidor spoke	191
Inicio y detención del servidor web	191
Reinicio del asistente de configuración inicial	192
Cambio del servidor concentrador	193
Restauración de la configuración a un estado de preconfiguración	193
Protección de aplicaciones, máquinas virtuales y sistemas	194
Adición de clientes	194
Selección del software de cliente y planificación de la instalación	195
Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	197
Visualización de políticas	198
Edición de políticas	198
Planificación de copia de seguridad y operaciones de archivado	199
Registro de clientes	200
Instalación y configuración de clientes	201
Configuración del cliente para ejecutar las operaciones planificadas	202
Configuración de comunicaciones a través de un cortafuegos	204
Gestión de operaciones de cliente	204
Evaluación de errores en registros de errores de cliente	205
Detención y reinicio del aceptador de cliente	205
Restablecimiento de contraseñas	206
Modificación del ámbito de una copia de seguridad de cliente	207
Gestión de actualizaciones del cliente	207
Poner fuera de servicio un nodo cliente	208
Desactivación de datos para liberar espacio de almacenamiento	210
Gestión del almacenamiento de datos	211
Auditoría de un contenedor de la agrupación de almacenamiento	211
Gestión de la capacidad de inventario	212
Gestión del uso de la memoria y del procesador	213
Ajuste de actividades planificadas	214

Gestión de la réplica	214
Compatibilidad de réplica	215
Habilitación de la réplica de nodo	215
Protección de datos en agrupaciones de almacenamiento de contenedor de directorios	216
Modificación de los valores de réplica	217
Establecimiento de distintas políticas de retención	218
Protección del servidor	219
Conceptos sobre la seguridad	219
Gestión de administradores	221
Cambio de los requisitos de contraseña	221
Protección de IBM Spectrum Protect en el sistema	222
Restricción del acceso de usuario al servidor	223
Limitación de acceso a través de restricciones de puerto	223
Detención e inicio del servidor	224
Detención del servidor	224
Inicio del servidor para tareas de mantenimiento o reconfiguración	225
Planificación para actualizar el servidor	226
Preparación para una parada	226
Implementación de un plan de recuperación tras desastre	227
Recuperación de pérdida de datos o de paradas del sistema	227
Restauración de la base de datos	230
Recuperación de datos dañados	231
Reparación de agrupaciones de almacenamiento	232
Solución de cinta	232
Planificación	233
Requisitos de planificación de cinta	234
Requisitos del sistema para una solución basada en cinta	234
Requisitos de hardware	235
Requisitos de software	238
Planificación de hojas de trabajo	239
Planificación del almacenamiento en disco	243
Planificación del almacenamiento en cinta	243
Dispositivos de cinta y bibliotecas soportados	244
Configuraciones de dispositivos de cinta soportadas	245
Movimiento de datos entre dispositivos de almacenamiento	245
Compartición de bibliotecas	246
Movimiento de datos sin LAN	246
Mezcla de tipos de dispositivos en una biblioteca	246
Diferentes generaciones de medios en una biblioteca	247
Mezcla de medios y agrupaciones de almacenamiento	248
Definiciones necesarias para dispositivos de almacenamiento en cinta	248
Planificación de la jerarquía de agrupaciones de almacenamiento	249
Almacenamiento de datos fuera del local	251
Planificación de la seguridad	251
Planificación de los roles de administración	252
Planificación para comunicaciones seguras	252
Planificación de almacenamiento de datos cifrados	253
Planificación del acceso de cortafuegos	253
Implementación	254
Configuración del sistema	255
Configuración del hardware de almacenamiento	256
Instalación del sistema operativo del servidor	256
Instalación en sistemas AIX	256
Instalación en sistemas Linux	258
Instalación en sistemas Windows	261
Configuración de E/S de la multivía de acceso	262
Sistemas AIX	262
Sistemas Linux	263

Sistemas Windows	264
Creación del ID de usuario para el servidor	265
Preparación de sistemas de archivos para el servidor	265
Sistemas AIX	265
Sistemas Linux	267
sistemas Windows	267
Instalación del servidor y Centro de operaciones	268
Instalación en sistemas AIX y Linux	268
Instalación en sistemas Windows	269
Configuración del servidor y el Centro de operaciones	269
Configuración de la instancia de servidor	270
Instalación del cliente de archivado y copia de seguridad	271
Configuración de opciones para el servidor	271
Conceptos sobre la seguridad	272
Configuración de Centro de operaciones	274
Registro de la licencia de producto	275
Definición de las reglas de retención de datos para su empresa	275
Definición de planificaciones para actividades de mantenimiento del servidor	276
Definición de planificaciones de cliente	280
Conexión de dispositivos de cinta para el servidor	280
Conectar un dispositivo de biblioteca automática a su dispositivo	280
Seleccionar un controlador de dispositivo de cinta	281
Controladores de dispositivos de cinta de IBM	281
Controladores de dispositivos de cinta de IBM Spectrum Protect	281
Nombres de archivo especiales para dispositivos de cinta	282
Instalación y configuración de controladores de dispositivos de cinta	283
Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM	283
Sistemas AIX	285
Dispositivos SCSI y de canal de fibra	285
Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores	286
Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta	286
Configuración de dispositivos conectados a SAN de canal de fibra	287
Sistemas Linux	287
Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas	288
Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfcp)	289
Información sobre los dispositivos SCSI del sistema	289
Impedir que las etiquetas de cinta se sobrescriban	289
sistemas Windows	290
Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta	290
Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta	291
Configuración de bibliotecas para su uso por parte de un servidor	292
Definición de dispositivos de cinta	293
Definición de bibliotecas y unidades	293
Definición de bibliotecas	293
Definición de unidades	294
Definición de las clases de dispositivo de cinta	295
Definición de las clases de dispositivo LTO	296
Combinación de unidades y medios LTO en una biblioteca	296
Límites de montaje en entornos de medios mixtos LTO	297
Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior	298
Definición de clases de dispositivo 3592	299
Combinación de generaciones de unidades y medios 3592 en una sola biblioteca	299
Control de las velocidades de acceso a datos en volúmenes 3592	300
Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior	301
Configuración de la compartición de bibliotecas	301
Ejemplo: Compartir biblioteca para servidores AIX y Linux	302
Ejemplo: compartición de bibliotecas para servidores Windows	304
Configuración del servidor gestor de bibliotecas	304

Configuración de los servidores cliente de biblioteca	305
Configuración de una jerarquía de agrupaciones de almacenamiento	306
Protección de aplicaciones y sistemas	307
Configuración del movimiento de datos sin LAN	308
Métodos de cifrado	308
Control de las operaciones de control de cintas	310
Cómo rellena volúmenes IBM Spectrum Protect	310
Especificar la capacidad estimada de los volúmenes de cinta	311
Especificación de formatos de grabación para soportes de cinta	311
Asociar objetos de biblioteca con clases de dispositivo	312
Control de las operaciones de montaje de medios para dispositivos de cinta	312
Control del número de volúmenes montados simultáneamente	312
Control de la cantidad de tiempo que un volumen permanece montado	313
Control de la cantidad de tiempo que un servidor espera una unidad	314
Operaciones de preferencia	314
Preferencia del punto de montaje	314
Preferencia de acceso a un volumen	315
Influencia de los cambios de dispositivo en la SAN	315
Visualización de la información de dispositivos	316
Medios de cinta Grabar una vez leer varias	316
Unidades preparadas para WORM	317
Incorporación de medios WORM	317
Restricciones en los medios WORM	318
Errores de montaje con medios WORM	318
Volver a etiquetar soportes WORM	318
Eliminar volúmenes WORM privados de una biblioteca	318
Creación de volúmenes DLT WORM	318
Soporte para cintas 3592 WORM cortas y normales	318
Consultar a una clase de dispositivo el valor del parámetro WORM	319
Resolución de problemas con dispositivos	319
Finalización de la implementación	320
Supervisión	320
Lista de comprobación diaria	320
Lista de comprobación periódica	327
Supervisión de los mensajes de alerta de cinta sobre errores de hardware	334
Prevenir errores causados por la incompatibilidad de los medios	334
Operaciones con cartuchos limpiadores	334
Verificación de la conformidad de licencia	335
Seguimiento del estado del sistema mediante informes de correo electrónico	336
Gestión	337
Gestión del Centro de operaciones	337
Gestión de operaciones de cliente	338
Evaluación de errores en registros de errores de cliente	338
Detención y reinicio del aceptador de cliente	339
Restablecimiento de contraseñas	340
Gestión de actualizaciones del cliente	340
Poner fuera de servicio un nodo cliente	341
Desactivación de datos para liberar espacio de almacenamiento	343
Gestión del almacenamiento de datos	343
Gestión de la capacidad de inventario	344
Ajuste de actividades planificadas	345
Optimización de operaciones habilitando la función de proximidad de los archivos de cliente	346
Efectos de la proximidad en las operaciones	347
Selección de volúmenes con proximidad habilitada	349
Selección de volúmenes con proximidad inhabilitada	350
Valores de proximidad	351
Proximidad de agrupaciones de almacenamiento de copias	351
Planificación y activación de la función de proximidad	351

Gestión de dispositivos de cinta	353
Preparación de medios extraíbles	353
Etiquetado de volúmenes de cinta	354
Dar de alta volúmenes de almacenamiento en una biblioteca	354
Incorporar un volumen en una biblioteca SCSI	356
Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca	356
Incorporación de volúmenes de almacenamiento desde los puertos de entrada/salida de la biblioteca	356
Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas	357
Incorporación de volúmenes	357
Comprobación de volúmenes en una biblioteca completa con intercambio	358
Volúmenes privados y volúmenes reutilizables	358
Direcciones de elementos para las ranuras de almacenamiento de biblioteca	359
Gestión del inventario de volúmenes	359
Control de acceso a volúmenes	359
Reutilización de cintas	360
Mantenimiento de un suministro de volúmenes reutilizables	361
Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM	362
Gestión del inventario de volumen en bibliotecas automatizadas	362
Cambiar el estado de un volumen de una biblioteca automatizada	363
Eliminación de volúmenes de una biblioteca automatizada	363
Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada	364
Gestión de una ubicación de desbordamiento	364
Auditoría de inventarios de volúmenes	365
Volúmenes grabados parcialmente	366
Operaciones con bibliotecas compartidas	366
Solicitudes del servidor para los volúmenes	367
Gestión de unidades de cinta	369
Actualización de unidades	369
Validación de datos durante operaciones de lectura/escritura en cinta	370
Unidades soportadas	371
Habilitación e inhabilitación de la protección de bloques lógicos	371
Operaciones de lectura/escritura en volúmenes	372
Gestión de agrupaciones de almacenamiento en una biblioteca de cintas	373
Limpieza de unidades de cinta	373
Métodos para limpiar unidades de cinta	374
Configuración del servidor para la limpieza de unidades en una biblioteca automatizada	375
Incorporar un cartucho limpiador en una biblioteca	376
Operaciones con cartuchos limpiadores	334
Resolución de errores relacionados con la limpieza de unidades	376
Sustitución de unidades de cinta	377
Suprimir unidades de cinta	377
Sustitución de las unidades con otras del mismo tipo	378
Migración de datos a unidades actualizadas	378
Protección del servidor	379
Gestión de administradores	379
Cambio de los requisitos de contraseña	380
Protección del servidor en el sistema	381
Detención e inicio del servidor	381
Detención del servidor	381
Inicio del servidor para tareas de mantenimiento o reconfiguración	382
Planificación para actualizar el servidor	383
Preparación para una parada	383
Preparación ante desastres y recuperación tras desastres mediante DRM	384
Archivo del plan de recuperación tras desastre	384
Recuperación de datos de cliente y servidor	387
Obtención de detalles de recuperación	388
Restauración de la base de datos	389
Archivos PDF	389

Servidores	390
Novedades	390
Actualizaciones del Centro de operaciones	391
Actualizaciones del servidor	392
Utilizar la creación de niveles de nube para la retención de datos de larga duración	392
Instalar IBM Spectrum Protect en Linux Ubuntu Server LTS	392
Mejorar la seguridad del entorno de almacenamiento	393
Tome medidas para proteger su sistema ante el ransomware	393
Notas del release V8.1	393
Servidores	393
Centro de operaciones	395
Dispositivos	396
Archivos léame V8.1 para los fixpacks	398
Instalación y actualización	398
Implementación de una solución IBM Spectrum Protect	398
Disponibilidad de las características por sistema operativo	398
Instalación y actualización del servidor	400
AIX: Instalación del servidor	401
AIX: Planificación para instalar el servidor de IBM Spectrum Protect	401
AIX: Qué debe saber primero	402
AIX: Planificación de rendimiento óptimo	402
AIX: Planificación del hardware del servidor y el sistema operativo	402
AIX: Planificación de discos de base de datos del servidor	405
AIX: Planificación de discos de registro de recuperación del servidor	407
AIX: Planificación de agrupaciones de almacenamiento de contenedores	408
AIX: Planificación de agrupaciones de almacenamiento DISK o FILE	414
AIX: Planificación de la tecnología de almacenamiento	416
AIX: Mejores métodos de instalación	418
AIX: Requisitos de sistema mínimos para sistemas AIX	420
AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema	422
AIX: IBM Installation Manager	423
AIX: Hojas de trabajo para planificar detalles para el servidor	424
AIX: Planificación de la capacidad	424
AIX: Requisitos de espacio de la base de datos	425
AIX: Número máximo de archivos	425
AIX: Capacidad de agrupación de almacenamiento	427
AIX: El gestor de bases de datos y el espacio temporal	427
AIX: Requisitos de espacio del registro de recuperación	428
AIX: Espacio del registro activo y archivado	428
AIX: Ejemplo: Operaciones básicas de almacén del cliente	429
AIX: Ejemplo: Varias sesiones de cliente	430
AIX: Ejemplo: Operaciones de grabación simultáneas	432
AIX: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	433
AIX: Ejemplo: Condiciones de variación extrema	433
AIX: Ejemplo: Copias de seguridad de base de datos completas	433
AIX: Ejemplo: Eliminación de datos duplicados	435
AIX: Espacio del duplicado de registro activo	439
AIX: Espacio del registro de migración tras error del archivo	439
AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	439
AIX: Supresión de archivos de retrotracción de instalación	440
AIX: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	441
AIX: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	441
AIX: Prácticas más adecuadas de denominación del servidor	441
AIX: Directorios de instalación para el servidor de IBM Spectrum Protect	443
AIX: Instalación de los componentes de servidor	443
AIX: Obtener el paquete de instalación	444
AIX: Utilización del asistente de instalación	444

AIX: Utilización del asistente de instalación de la consola	445
AIX: Utilización de modalidad silenciosa	446
AIX: Instalación de paquetes de idioma del servidor	447
AIX: Idiomas locales del servidor	447
AIX: Configuración de un paquete de idiomas	448
AIX: Actualización de un paquete de idiomas	448
AIX: Realización de los primeros pasos tras instalar la versión 8.1.3	449
AIX: Creación del ID de usuario y de directorios para la instancia del servidor	450
AIX: Configuración del servidor de IBM Spectrum Protect	451
AIX: Utilización del asistente de configuración	451
AIX: Utilización de los pasos de configuración manual	452
AIX: Creación de una instancia del servidor	452
AIX: Configuración de comunicaciones de servidor y cliente en sistemas UNIX	453
AIX: Establecimiento de opciones de TCP/IP	454
AIX: Establecimiento de opciones de memoria compartida	454
AIX: Configuración de las opciones de la capa de sockets seguros	455
AIX: Formateo de la base de datos y las anotaciones	455
AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	456
AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	457
AIX: Inicio de la instancia de servidor	458
AIX: Comprobación de los derechos de acceso y límites de usuario	459
AIX: Inicio del servidor con el ID de usuario de la instancia	460
AIX: Inicio automático de los servidores	461
AIX: Inicio del servidor en modalidad de mantenimiento	461
AIX: Detención del servidor	462
AIX: Registro de licencias	463
AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	463
AIX: Ejecución de varias instancias de servidor en un solo sistema	463
AIX: Supervisión del servidor	464
AIX: Instalación de un fixpack de IBM Spectrum Protect	465
AIX: Revertir de la versión 8.1.3 a un servidor anterior	467
AIX: Referencia: Mandatos de DB2 para bases de datos del servidor	469
AIX: Desinstalar IBM Spectrum Protect	471
AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	472
AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola	472
AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	473
AIX: Desinstalación e instalación de IBM Spectrum Protect	473
AIX: Desinstalación de IBM Installation Manager	474
Linux: Instalación del servidor	474
Linux: Planificación para instalar el servidor de IBM Spectrum Protect	475
Linux: Qué debe saber primero	475
Linux: Planificación de rendimiento óptimo	476
Linux: Planificación del hardware del servidor y el sistema operativo	476
Linux: Planificación de discos de base de datos del servidor	479
Linux: Planificación de discos de registro de recuperación del servidor	481
Linux: Planificación de agrupaciones de almacenamiento de contenedores	483
Linux: Planificación de agrupaciones de almacenamiento DISK o FILE	488
Linux: Planificación de la tecnología de almacenamiento	490
Linux: Mejores métodos de instalación	492
Linux: Requisitos mínimos del sistema para sistemas Linux	494
Linux: Requisitos mínimos del servidor Linux x86_64	494
Linux: Requisitos mínimos del servidor Linux on System z	496
Linux: Requisitos mínimos de servidor Linux on Power Systems (little endian)	498
Linux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema	499
Linux: IBM Installation Manager	500
Linux: Hojas de trabajo para planificar detalles para el servidor	501
Linux: Planificación de la capacidad	501
Linux: Requisitos de espacio de la base de datos	502

Linux: Número máximo de archivos	502
Linux: Capacidad de agrupación de almacenamiento	504
Linux: El gestor de bases de datos y el espacio temporal	504
Linux: Requisitos de espacio del registro de recuperación	505
Linux: Espacio del registro activo y archivado	505
Linux: Ejemplo: Operaciones básicas de almacén del cliente	506
Linux: Ejemplo: Varias sesiones de cliente	507
Linux: Ejemplo: Operaciones de grabación simultáneas	509
Linux: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	510
Linux: Ejemplo: Condiciones de variación extrema	510
Linux: Ejemplo: Copias de seguridad de base de datos completas	510
Linux: Ejemplo: Eliminación de datos duplicados	512
Linux: Espacio del duplicado de registro activo	516
Linux: Espacio del registro de migración tras error del archivo	516
Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	516
Linux: Supresión de archivos de retrotracción de instalación	517
Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	518
Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	518
Linux: Prácticas más adecuadas de denominación del servidor	518
Linux: Directorios de instalación para el servidor de IBM Spectrum Protect	520
Linux: Instalación de los componentes de servidor	520
Linux: Obtener el paquete de instalación	521
Linux: Utilización del asistente de instalación	521
Linux: Utilización del asistente de instalación de la consola	522
Linux: Utilización de modalidad silenciosa	523
Linux: Instalación de paquetes de idioma del servidor	523
Linux: Idiomas locales del servidor	524
Linux: Configuración de un paquete de idiomas	525
Linux: Actualización de un paquete de idiomas	525
Linux: Realización de los primeros pasos tras instalar la versión 8.1.3	525
Linux: Ajuste de parámetros del kernel en sistemas Linux	526
Linux: Actualización de parámetros	527
Linux: Valores recomendados	527
Linux: Creación del ID de usuario y de directorios para la instancia del servidor	527
Linux: Configuración del servidor de IBM Spectrum Protect	529
Linux: Utilización del asistente de configuración	529
Linux: Utilización de los pasos de configuración manual	529
Linux: Creación de una instancia del servidor	530
Linux: Configuración de comunicaciones de servidor y cliente en sistemas UNIX	531
Linux: Establecimiento de opciones de TCP/IP	532
Linux: Establecimiento de opciones de memoria compartida	532
Linux: Configuración de las opciones de la capa de sockets seguros	533
Linux: Formateo de la base de datos y las anotaciones	533
Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	534
Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	535
Linux: Inicio de la instancia de servidor	536
Linux: Comprobación de los derechos de acceso y límites de usuario	537
Linux: Inicio del servidor con el ID de usuario de la instancia	538
Linux: Inicio automático de los servidores en sistemas Linux	539
Linux: Inicio del servidor en modalidad de mantenimiento	540
Linux: Detención del servidor	541
Linux: Registro de licencias	541
Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	541
Linux: Ejecución de varias instancias de servidor en un solo sistema	542
Linux: Supervisión del servidor	542
Linux: Instalación de un fixpack de IBM Spectrum Protect	543
Linux: Revertida de la versión 8.1.3 a un servidor anterior	545
Linux: Referencia: Mandatos de DB2 para bases de datos del servidor	547

Linux: Desinstalar IBM Spectrum Protect	550
Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	550
Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola	551
Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	551
Linux: Desinstalación e instalación de IBM Spectrum Protect	552
Linux: Desinstalación de IBM Installation Manager	552
Windows: Instalación del servidor	553
Windows: Planificación para instalar el servidor de IBM Spectrum Protect	553
Windows: Qué debe saber primero	554
Windows: Planificación de rendimiento óptimo	554
Windows: Planificación del hardware del servidor y el sistema operativo	555
Windows: Planificación de discos de base de datos del servidor	557
Windows: Planificación de discos de registro de recuperación del servidor	559
Windows: Planificación de agrupaciones de almacenamiento de contenedores	560
Windows: Planificación de agrupaciones de almacenamiento DISK o FILE	566
Windows: Planificación de la tecnología de almacenamiento	568
Windows: Mejores métodos de instalación	570
Windows: Requisitos mínimos del sistema para sistemas Windows	572
Windows: IBM Installation Manager	574
Windows: Hojas de trabajo para planificar detalles para el servidor	575
Windows: Planificación de la capacidad	575
Windows: Requisitos de espacio de la base de datos	576
Windows: Número máximo de archivos	576
Windows: Capacidad de agrupación de almacenamiento	578
Windows: El gestor de bases de datos y el espacio temporal	578
Windows: Requisitos de espacio del registro de recuperación	579
Windows: Espacio del registro activo y archivado	579
Windows: Ejemplo: Operaciones básicas de almacén del cliente	580
Windows: Ejemplo: Varias sesiones de cliente	581
Windows: Ejemplo: Operaciones de grabación simultáneas	583
Windows: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	584
Windows: Ejemplo: Condiciones de variación extrema	584
Windows: Ejemplo: Copias de seguridad de base de datos completas	584
Windows: Ejemplo: Eliminación de datos duplicados	586
Windows: Espacio del duplicado de registro activo	590
Windows: Espacio del registro de migración tras error del archivo	590
Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	590
Windows: Supresión de archivos de retrotracción de instalación	591
Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	592
Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	592
Windows: Prácticas más adecuadas de denominación del servidor	592
Windows: Directorios de instalación para el servidor de IBM Spectrum Protect	593
Windows: Instalación de los componentes de servidor	594
Windows: Obtener el paquete de instalación	594
Windows: Utilización del asistente de instalación	595
Windows: Utilización del asistente de instalación de la consola	596
Windows: Utilización de modalidad silenciosa	596
Windows: Instalación de paquetes de idioma del servidor	597
Windows: Idiomas locales del servidor	597
Windows: Configuración de un paquete de idiomas	598
Windows: Actualización de un paquete de idiomas	598
Windows: Realización de los primeros pasos tras instalar la versión 8.1.3	598
Windows: Creación del ID de usuario y de directorios para la instancia del servidor	599
Windows: Configuración del servidor de IBM Spectrum Protect	601
Windows: Utilización del asistente de configuración	601
Windows: Utilización de los pasos de configuración manual	602
Windows: Creación de una instancia del servidor	602
Windows: Configuración de comunicaciones en sistemas Windows	603

Windows: Establecimiento de opciones de TCP/IP	604
Windows: Establecimiento de opciones de Named Pipes	604
Windows: Configuración de las opciones de la capa de sockets seguros	605
Windows: Formateo de la base de datos y las anotaciones	605
Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	606
Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	607
Windows: Inicio de la instancia del servidor en sistemas Windows	607
Windows: Configuración del servidor para que se inicie como un servicio de Windows	608
Windows: Inicio del servidor como un servicio de Windows.	609
Windows: Creación manual y configuración de un servicio de Windows	610
Windows: Inicio del servidor en segundo plano	610
Windows: Servicios asociados al servidor en sistemas Windows	611
Windows: Inicio del servidor en modalidad de mantenimiento	611
Windows: Detención del servidor	612
Windows: Registro de licencias	612
Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	612
Windows: Ejecución de varias instancias de servidor en un solo sistema	613
Windows: Supervisión del servidor	613
Windows: Instalación de un fixpack de IBM Spectrum Protect	614
Windows: Revertir de la versión 8.1.3 a un servidor anterior	616
Windows: Referencia: Mandatos de DB2 para bases de datos del servidor	618
Windows: Desinstalar IBM Spectrum Protect	621
Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	622
Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola	622
Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	623
Windows: Desinstalación e instalación de IBM Spectrum Protect	623
Windows: Desinstalación de IBM Installation Manager	624
Actualización del servidor a la versión 8.1	624
Actualización a V8.1	625
Planificación de la actualización	626
Preparación del sistema	626
Instalación del servidor y comprobación de la actualización	629
Actualización del servidor en un entorno en clúster	633
Actualización de V6.3 o V7.1 a V8.1.3 en un entorno en clúster para AIX con una instancia de base de datos compartida	634
Actualización de V6.3 a V8.1.3 en un entorno en clúster para AIX con instancias de base de datos independientes	636
Actualización de V8.1.3 en un entorno en clúster para Linux	638
Actualización de V6.3 o V7.1 a V8.1.3 en un entorno en clúster para Windows	638
Instalación y actualización del Centro de operaciones	639
Planificación para instalar el Centro de operaciones	640
Requisitos del sistema del Centro de operaciones	641
Requisitos de sistema del Centro de operaciones	642
Requisitos del servidor concentrador y spoke	642
Consejos para designar la configuración del servidor concentrador y el servidor de radio	643
Consejos para elegir un servidor concentrador	644
Requisitos de sistema operativo	645
Requisitos del navegador web	645
Requisitos de idioma	646
Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect	647
Los ID de administrador que requiere el centro de operaciones	648
IBM Installation Manager	649
Lista de comprobación de la instalación	649
Instalar el Centro de operaciones	651
Obtención del paquete de instalación de Centro de operaciones	652
Instalación de Centro de operaciones utilizando el asistente gráfico	652
Instalar el Centro de operaciones en modalidad de consola	653
Instalación de Centro de operaciones en el modo silencioso	654
Actualización del Centro de operaciones	654
Guía de inicio de la Centro de operaciones	655

Configurar el Centro de Operaciones	656
Designar el servidor central	656
Adición de un servidor de radio	657
Envío de alertas por correo electrónico a los administradores	657
Adición de texto personalizado a la pantalla de inicio de sesión	659
Habilitación de servicios REST	660
Configuración para la comunicación segura	660
Entre el Centro de operaciones y el servidor concentrador	660
Entre el servidor concentrador y un servidor de radio	662
Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones	664
Iniciar y detener el servidor web	665
Apertura del Centro de operaciones	666
Recopilación de información de diagnóstico con el servicio de gestión de clientes	666
Instalación de servicio de gestión de clientes utilizando el asistente gráfico	667
Instalación de servicio de gestión de clientes en modalidad silenciosa	668
Verificación de la instalación	669
Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes	670
Inicio y detención del servicio de gestión de clientes	670
Desinstalación de servicio de gestión de clientes	671
Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas	671
Resolución de problemas de la instalación de Centro de operaciones	672
El asistente de instalación gráfica no puede iniciarse en un sistema AIX	672
Las letras en chino, japonés o coreano se muestran incorrectamente	672
Desinstalación de Centro de operaciones	672
Desinstalación de Centro de operaciones utilizando el asistente gráfico	673
Desinstalación del Centro de operaciones en modalidad de consola	673
Desinstalar Centro de operaciones en modalidad silenciosa	673
Volver a una versión anterior de Centro de operaciones	674
Configuración de servidores	674
Protección del servidor	676
Conceptos sobre la seguridad	677
Gestión de administradores	679
Cambio de los requisitos de contraseña	679
Protección de IBM Spectrum Protect en el sistema	680
Restricción del acceso de usuario al servidor	681
Limitación de acceso a través de restricciones de puerto	681
Protección del entorno de almacenamiento contra el ransomware	682
Protección de las comunicaciones	682
Comunicación SSL y TLS	683
Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL	685
Configuración del servidor para aceptar conexiones SSL	685
Configuración de clientes para comunicarse con el servidor utilizando SSL	687
Configuración del servidor para conectarse a otro servidor utilizando SSL	687
Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL	688
Configuración de un agente de almacenamiento para utilizar SSL	688
Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL	689
Autenticación de los usuarios mediante un servidor LDAP	689
Réplica de datos de cliente en otro servidor	689
Compatibilidad de réplica	690
Habilitación de la réplica de nodo	691
Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio	692
Modificación de los valores de réplica	693
Establecimiento de distintas políticas de retención	693
Configuración de entornos en clúster	694
Visión general del entorno en clúster	695
entorno en clúster de AIX	695
Requisitos del clúster	696

Recuperación de errores y restablecimiento de PowerHA	697
Instalación y configuración de PowerHA SystemMirror para AIX	697
Instalación y configuración del clúster	697
Configuración del nodo primario	698
Configuración de un nodo secundario con una instancia de DB2 compartida	698
Configuración de un nodo secundario con una instancia de DB2 independiente	699
Instalación del servidor en un nodo de producción	700
Instalación del cliente en un nodo de producción	701
Verificación de la configuración del servidor	701
Configurar el nodo de espera	702
Definición de los dispositivos de almacenamiento de medios extraíbles	702
Configuración del gestor de clúster	703
Resolución de problemas del entorno en clúster de PowerHA	703
entorno en clúster de Linux	703
Descripción de un entorno en clúster de dos nodos	704
Topología de disco compartido de dos nodos	706
Grupos de recursos de Tivoli System Automation	707
Configuración de un clúster	708
Requisitos previos para la configuración de un entorno en clúster	709
Instalación y configuración de componentes	709
Instalación de componentes de servidor	709
Configuración del nodo primario	709
Configuración del nodo secundario	710
Instalación de Tivoli System Automation	711
Creación de una etiqueta para los puntos de montaje	711
Instalación y configuración de Tivoli System Automation	712
Preparación para activar los nodos de clúster para el dominio	712
Configuración de recursos del grupo de volúmenes	712
Configuración de recursos que no están en un grupo de volúmenes	713
Activación de la política base	714
Adición de puntos de montaje a directorios	714
Configuración de recursos de almacenamiento	715
Adición de una agrupación de almacenamiento	715
Eliminar una agrupación de almacenamiento	716
Eliminación de un punto de montaje	716
Actualización del servidor que es un Tivoli System Automation configurado	717
entorno en clúster de Windows	717
Visión general del entorno de Microsoft Failover Cluster	718
Recuperación de errores de cinta para los nodos de un clúster	720
Planificación de un entorno en clúster	720
Hoja de trabajo de configuración del clúster	720
Planificación de la configuración de hardware y software del clúster	721
Configuración de IBM Spectrum Protect en Microsoft Failover Cluster	722
Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster	722
Preparación de un grupo de recursos de clúster para un servidor virtual	723
Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster	723
Inicialización del servidor en el nodo primario	724
Verificación de la configuración en un Microsoft Failover Cluster	724
Prueba de migración tras error	724
Mantenimiento del entorno en clúster	725
Migración de un servidor existente en un clúster	725
Añadir un servidor utilizando copia de seguridad y restauración	725
Gestión de un servidor virtual en un clúster	726
Gestión de la recuperación de errores de cinta	726
Resolución de problemas con las anotaciones de clúster	726
Configuración de clientes	727
Adición de clientes	727
Selección del software de cliente y planificación de la instalación	728

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	729
Visualización de políticas	730
Edición de políticas	730
Planificación de copia de seguridad y operaciones de archivado	732
Registro de clientes	732
Instalación y configuración de clientes	733
Configuración del cliente para ejecutar las operaciones planificadas	734
Configuración de comunicaciones a través de un cortafuegos	736
Planificación de actualizaciones de cliente	737
Personalización de políticas	738
Conceptos de políticas	739
Retención y caducidad de las versiones de copia de seguridad	740
Caducidad de archivos y procesamiento de la caducidad	741
Ejemplo: Retención cuando una política utiliza solo controles temporales	741
Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión	742
Interacciones entre configuraciones de política	744
Activación de las políticas después de las actualizaciones	745
Personalización de una política	747
Creación de una política copiando una política existente	748
Creación de un dominio de políticas	749
Control de las operaciones de cliente mediante conjuntos de opciones de cliente	750
Configuración del almacenamiento	751
Tipos de agrupaciones de almacenamiento	751
Opciones de eliminación de datos duplicados	755
Configuración de dispositivos de almacenamiento	756
Configuración de una agrupación de almacenamiento de contenedores de directorios	756
Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta	757
Rotación de volúmenes de cinta fuera del local sin DRM	759
Cambiar el umbral de reclamación de volumen	760
Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor	760
Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro	761
Configuración de una agrupación de almacenamiento de contenedores en la nube	763
Preparación para Amazon con S3 (fuera del local)	765
Preparación de un dispositivo compatible con Amazon S3	766
Preparación para Microsoft Azure (fuera del local)	766
Preparación para IBM Cloud Object Storage con Swift (fuera del local)	767
Preparación para IBM Cloud Object Storage con S3 (fuera del local)	768
Preparación para IBM Cloud Object Storage con S3 (en local)	769
Preparación para OpenStack con Swift	770
Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube	771
Definición de una regla de almacenamiento para los niveles en la nube	771
Optimización de rendimiento para almacenamiento de objetos en la nube	772
Gestión de agrupaciones de almacenamiento de contenedores	772
Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor	774
Limpieza de los datos de una agrupación de almacenamiento de origen	776
Auditoría de un contenedor de la agrupación de almacenamiento	776
Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos	777
Supervisión de soluciones de almacenamiento	778
Lista de comprobación diaria	779
Lista de comprobación periódica	786
Verificación de la conformidad de licencia	792
Seguimiento del estado del sistema mediante informes de correo electrónico	793
Selección, configuración y uso de herramientas de supervisión	794
Gestión de operaciones	796
Gestión de operaciones del servidor	797
Detención e inicio del servidor	797
Detención del servidor	797
Inicio del servidor para tareas de mantenimiento o reconfiguración	798

Gestión de la capacidad de inventario	799
Gestión del uso de la memoria y del procesador	801
Determinación de si Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema	801
Planificación de la actualización del servidor	803
Ajuste de actividades planificadas	803
Gestión de operaciones de cliente	804
Modificación del ámbito de una copia de seguridad de cliente	804
Evaluación de errores en registros de errores de cliente	805
Detención y reinicio del aceptador de cliente	805
Restablecimiento de contraseñas	806
Poner fuera de servicio un nodo cliente	807
Desactivación de datos para liberar espacio de almacenamiento	809
Gestión de actualizaciones del cliente	809
Gestión del Centro de operaciones	810
Adición y eliminación de servidores spoke	811
Adición de un servidor de radio	811
Eliminación de un servidor spoke	811
Inicio y detención del servidor web	812
Reinicio del asistente de configuración inicial	813
Cambio del servidor concentrador	813
Restauración de la configuración a un estado de preconfiguración	814
Configuración de bibliotecas de cintas virtuales	815
Consideraciones sobre el uso de las bibliotecas de cintas virtuales	815
Capacidad de almacenamiento para las bibliotecas de cintas virtuales	816
Configuración de unidades para las bibliotecas de cintas virtuales	816
Agregar una biblioteca de cintas virtuales a su entorno	816
Definir todas las unidades y vías de acceso de una biblioteca	817
Ejemplo: biblioteca SCSI o VTL con un único tipo de dispositivo de unidad	818
Ejemplo: Biblioteca VTL o SCSI con varios tipos de dispositivos de unidad	819
Protección de servidores de archivos NAS	821
Requisitos de NDMP	822
Interfaces para operaciones NDMP	823
Formatos de datos para operaciones de copia de seguridad NDMP	823
Gestión de operaciones NDMP	824
Gestión de los nodos del servidor de archivos NAS	824
Gestión de los transportadores de datos utilizados en las operaciones NDMP	825
Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP	826
Gestión de agrupaciones de almacenamiento para operaciones NDMP	826
Gestión de tablas de contenido	827
Impedir que las conexiones NDMP inactivas se cierren	827
Habilitar el estado activo de TCP	828
Especificar tiempo de inactividad de conexión (AIX, Linux y Windows)	828
Configuración de IBM Spectrum Protect para operaciones NDMP	828
En un entorno no de clúster	828
Configuración de una política de IBM Spectrum Protect para operaciones NDMP	830
Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect	831
Políticas para copias de seguridad iniciadas con la interfaz de cliente	831
Determinación de la ubicación de copia de seguridad NAS	832
Bibliotecas y unidades de cintas para operaciones NDMP	833
Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS	834
Configuración de una biblioteca de cintas para operaciones NDMP	836
Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS	837
Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect	838
Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS	840
Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect	841
Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect	843
Registro de nodos NAS con el servidor de IBM Spectrum Protect	844
Definición de un transportador de datos para un servidor de archivos de NAS	845

Definición de vías de acceso para operaciones NDMP	845
Definición de vías de acceso a unidades	846
Unidades conectadas a un servidor de archivos y al servidor de IBM Spectrum Protect	846
Unidades conectadas únicamente a un servidor de archivos	847
Obtención de nombres para dispositivos conectados a un servidor de archivos	847
Definición de vías de acceso a bibliotecas	848
Planificación de operaciones NDMP	849
Definición de espacios de archivos virtuales	849
Copia de seguridad de datos mediante la función de cinta a cinta	850
Traslado de datos con la función de copia de cinta a cinta	850
En un entorno en clúster de NetApp	850
Configuración de copias de seguridad de clúster completo en dispositivos de cinta	852
Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect	854
Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect	855
Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster	856
Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP	859
Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único	859
Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect	860
Copia de seguridad y restauración en nivel de archivo para operaciones NDMP	861
Interfaces para las operaciones de restauración a nivel de archivos	862
Caracteres internacionales para servidores de archivos NetApp	862
Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio	863
Operaciones de copia de seguridad y restauración a nivel de directorio	863
Copia de seguridad y restauración a nivel de directorio para operaciones NDMP	863
Copia de seguridad y restauración con instantáneas	864
Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape	864
Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra	865
Réplica de los nodos NAS	865
Protección de datos con la característica NetApp SnapLock	866
Reclamación y la característica SnapLock	867
Periodos de retención	867
Configuración de la característica SnapLock para la retención basada en sucesos	869
Protección de datos continua con la característica SnapLock	870
Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect	870
Reparación y recuperación de datos	870
Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino	871
Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor	873
Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor	875
Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino	876
Recuperación después de un siniestro	877
Reparación desde volúmenes de agrupación de almacenamiento de copia de contenedor	877
Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino	878
Reparación de un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor	879
Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado	881
Mandatos, opciones y programas de utilidad del servidor	881
Gestión del servidor desde la línea de mandatos	882
Emisión de mandatos del cliente de administración	883
Inicio y detención del cliente de administración	883
Supervisión de actividades del servidor desde el cliente de administración	884
Supervisión de montajes de medios extraíbles del cliente de administración	884
Proceso de mandatos individuales desde el cliente de administración	884
Proceso de una serie de mandatos del cliente de administración	885
Formateo de la salida de los mandatos	885
Cómo guardar la salida del mandato en una ubicación especificada	885
Opciones de cliente de administración	886
Emisión de mandatos desde el Centro de operaciones	888
Emisión de mandatos desde la consola del servidor	888

Especificación de mandatos de administración	888
Lectura de los diagramas de sintaxis	889
Utilización de caracteres de continuación para entrar mandatos largos	892
Denominación de objetos de IBM Spectrum Protect	893
Utilización de caracteres comodín para especificar nombres de objetos	893
Especificación de descripciones en parámetros de palabra clave	894
Control del proceso de mandatos	895
Proceso de mandatos de servidor	895
Detener procesos en segundo plano	896
Realización de tareas simultáneamente en varios servidores	896
Clases de privilegio	898
Mandatos que requieren privilegio de sistema	898
Mandatos que requieren privilegio de políticas	901
Mandatos que requieren privilegio de almacenamiento	901
Mandatos que requieren privilegio de operador	902
Mandatos que puede emitir cualquier administrador	902
Mandatos de administración	903
ACCEPT DATE (aceptar la fecha del sistema actual)	907
ACTIVATE POLICYSET (Activar un nuevo juego de políticas)	908
ASSIGN DEFMGMTCLASS (asignar una clase de gestión predeterminada)	909
Mandatos AUDIT	910
Mandatos AUDIT CONTAINER	910
Auditoría de contenedor de nubes	910
Auditoría de un contenedor de directorios	915
AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)	919
AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)	920
AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)	922
AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)	923
AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)	924
Mandatos BACKUP	928
BACKUP DB (copia de seguridad de la base de datos)	928
BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)	933
BACKUP NODE (Copia de seguridad de un nodo NAS)	935
BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)	938
BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)	941
BEGIN EVENTLOGGING (Iniciar anotación de eventos)	942
Mandatos CANCEL	944
CANCEL EXPIRATION (Cancelar un proceso de caducidad)	944
CANCEL EXPORT (Suprimir una operación de exportación suspendida)	944
CANCEL PROCESS (Cancelar un proceso de administración)	945
CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)	947
CANCEL REQUEST (Cancelar una o más peticiones de montaje)	948
CANCEL RESTORE (Cancelar una sesión de restauración reinicializable)	948
CANCEL SESSION (Cancelar una o más sesiones cliente)	949
CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)	950
CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)	955
CLEAN DRIVE (Limpiar una unidad)	959
COMMIT (controlar la validación de mandatos en una macro)	960
CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)	961
Mandatos COPY	962
COPY ACTIVE DATA (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)	963
COPY CLOPTSET (Copiar un conjunto de opciones de cliente)	965
COPY DOMAIN (Copiar un dominio de políticas)	966
COPY MGMTCLASS (Copiar una clase de gestión)	967
COPY POLICYSET (Copiar un juego de políticas)	968
COPY PROFILE (Copiar un perfil)	969

COPY SCHEDULE (Copiar una planificación de cliente o de mandato de administración)	970
COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)	971
COPY SCHEDULE (Crear una copia de una planificación para las operaciones de administración)	971
COPY SCRIPT (copiar un script de IBM Spectrum Protect)	972
COPY SERVERGROUP (Copiar un grupo de servidores)	973
DEACTIVATE DATA (Desactivar datos para un nodo de cliente)	974
Mandatos DECOMMISSION	975
DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)	976
DECOMMISSION VM (Poner fuera de servicio una máquina virtual)	977
Mandatos DEFINE	978
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	979
DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)	981
DEFINE BACKUPSET (Definir un juego de copias de seguridad)	982
DEFINE CLIENTACTION (Definir una acción de cliente única)	985
DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)	989
DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)	991
DEFINE COLLOGROUP (Definir un grupo de proximidad)	992
DEFINE COLLOCMEMBER	993
DEFINE COPYGROUP (Definir un grupo de copia)	995
DEFINE COPYGROUP (Definir un grupo de copia de seguridad)	996
DEFINE COPYGROUP (Definir un grupo de copias archivadas)	999
DEFINE DATAMOVER (Definir un transportador de datos)	1002
DEFINE DEVCLASS (Definir una clase de dispositivo)	1004
3590	1005
3592	1008
4MM	1013
8MM	1016
Centera	1020
DLT	1022
Ecartridge	1026
Archivo	1031
Generictape	1033
LTO	1035
NAS	1040
Removablefile	1042
Servidor	1043
VolSafe	1045
DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS)	1048
3590, para el servidor de medios de z/OS	1049
3592, para el servidor de medios de z/OS	1052
ECARTRIDGE, para el servidor de medios de z/OS	1056
FILE, para el servidor de medios de z/OS	1061
DEFINE DOMAIN (Definir un nuevo dominio de políticas)	1063
DEFINE DRIVE (Definir una unidad en una biblioteca)	1064
DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)	1068
DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)	1069
DEFINE LIBRARY (Definir una biblioteca)	1070
349X	1071
ACSLs	1073
EXTERNAL	1076
FILE	1077
MANUAL	1078
SCSI	1079
Compartido	1082
VTL	1083
ZOSMEDIA	1085
DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)	1086
DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)	1087

DEFINE MGMTCLASS (Definir una clase de gestión)	1088
DEFINE NODEGROUP (Definir un grupo de nodos)	1090
DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)	1091
DEFINE PATH (Definir una ruta)	1092
El destino es una unidad	1093
El destino es una biblioteca	1098
El destino es una biblioteca ZOSMEDIA	1100
DEFINE POLICYSET (Definir un juego de políticas)	1101
DEFINE PROFASSOCIATION (Definir una asociación de perfil)	1102
DEFINE PROFILE (Definir un perfil)	1106
DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)	1107
DEFINE RECOVERYMEDIA (Definir medio de recuperación)	1108
DEFINE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)	1109
DEFINE SCHEDULE (Definir una planificación de cliente)	1110
DEFINE SCHEDULE (Definir una planificación para un mandato de administración)	1120
DEFINE SCRATCHPADENTRY (Definir una entrada de registro)	1127
DEFINE SCRIPT (definir un script de IBM Spectrum Protect)	1128
DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)	1129
DEFINE SERVERGROUP (Definir un grupo de nodo)	1136
DEFINE SPACETRIGGER (Definir desencadenante de espacio)	1137
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	1139
DEFINE STGPOOL (Definir una agrupación de almacenamiento)	1142
Agrupación de almacenamiento de contenedores en la nube	1143
Agrupación de almacenamiento de contenedores de directorio	1147
Agrupación de almacenamiento de copia de contenedor	1152
Agrupación de acceso aleatorio primaria	1155
Agrupación de acceso secuencial primaria	1162
Agrupación de copias	1176
Agrupación de datos activos	1182
DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)	1188
DEFINE STGRULE (Definir una regla de almacenamiento para agrupaciones de almacenamiento)	1190
DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)	1192
DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)	1193
DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)	1194
Mandatos DELETE	1200
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	1201
DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)	1202
DELETE BACKUPSET (Suprimir un juego de copias de seguridad)	1203
DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)	1206
DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)	1207
DELETE COLLOGROUP (Suprimir un grupo de proximidad)	1208
DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)	1209
DELETE COPYGROUP (Suprimir un grupo de copias de seguridad o de archivado)	1211
DELETE DATAMOVER (Suprimir un transportador de datos)	1212
DELETE DEDUPSTATS (Suprimir las estadísticas de eliminación de duplicados de datos)	1213
DELETE DEVCLASS (Suprimir una clase de dispositivo)	1216
DELETE DOMAIN (Suprimir un dominio de políticas)	1216
DELETE DRIVE (Suprimir una unidad de una biblioteca)	1217
DELETE EVENT (Suprimir registros de eventos)	1218
DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)	1220
DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)	1220
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	1223
DELETE LIBRARY (Suprimir una biblioteca)	1224
DELETE MACHINE (Suprimir información de una máquina)	1225
DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)	1226
DELETE MGMTCLASS (Suprimir una clase de gestión)	1226
DELETE NODEGROUP (Suprimir un grupo de nodos)	1227
DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)	1228

DELETE PATH (Suprimir una ruta)	1229
DELETE POLICYSET (Suprimir un juego de políticas)	1230
DELETE PROFASSOCIATION (Suprimir una asociación de perfil)	1231
DELETE PROFILE (Suprimir un perfil)	1233
DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)	1234
DELETE RECOVERYMEDIA (Suprimir medio de recuperación)	1235
DELETE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)	1235
DELETE SCHEDULE (Suprimir una planificación de cliente)	1236
DELETE SCHEDULE (Suprimir una planificación de administración)	1236
DELETE SCRATCHPADENTRY (Suprimir una entrada de registro)	1237
DELETE SCRIPT (Suprimir líneas de mandatos de un script o suprimir todo el script)	1238
DELETE SERVER (Suprimir una definición de servidor)	1238
DELETE SERVERGROUP (Suprimir un grupo de servidores)	1239
DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)	1240
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	1240
DELETE STGPOOL (Suprimir una agrupación de almacenamiento)	1241
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)	1243
DELETE STGRULE (Suprimir reglas de almacenamiento para agrupaciones de almacenamiento)	1244
DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)	1244
DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)	1245
DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)	1246
DELETE VOLHISTORY (Suprimir información histórica de volúmenes)	1247
DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)	1251
Mandatos DISABLE	1253
DISABLE EVENTS (Desactivar eventos para anotación de eventos)	1253
DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)	1256
DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)	1256
Mandatos DISMOUNT	1258
DISPLAY OBJNAME (Mostrar un nombre de objeto completo)	1258
Mandatos ENABLE	1259
ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)	1259
ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)	1261
ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)	1262
ENCRYPT STGPOOL (Cifrar datos en una agrupación de almacenamiento)	1264
END EVENTLOGGING (Detener eventos de anotaciones)	1265
EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)	1266
Mandatos EXPORT	1269
EXPORT ADMIN (Exportar información del administrador)	1270
EXPORT ADMIN (Exportar definiciones del administrador a medios secuenciales)	1271
EXPORT ADMIN (Exportar información del administrador directamente a otro servidor)	1274
EXPORT NODE (Exportar información de nodos cliente)	1275
EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)	1277
EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)	1284
EXPORT POLICY (Exportar información de políticas)	1291
EXPORT POLICY (Exportar información de política a medios secuenciales)	1292
EXPORT POLICY (Exportar una política directamente a otro servidor)	1294
EXPORT SERVER (Exportar información del servidor)	1295
EXPORT SERVER (Exportar un servidor a medios secuenciales)	1297
EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)	1303
EXTEND DBSPACE (Incrementar el espacio para la base de datos)	1309
Mandatos GENERATE	1311
GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)	1311
GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)	1317
GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)	1319
Mandatos GRANT	1321
GRANT AUTHORITY (agregar autorización de administrador)	1321
GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)	1324
HALT (Concluir el servidor)	1325

HELP (Obtener ayuda sobre mandatos y mensajes de error)	1326
IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)	1328
Mandatos IMPORT	1331
IMPORT ADMIN (Importar información del administrador)	1331
IMPORT NODE (Importar información de nodos clientes)	1334
IMPORT POLICY (Importar información de políticas)	1339
IMPORT SERVER (Importar información del servidor)	1342
INSERT MACHINE (Insertar información de características o instrucciones de recuperación)	1346
ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)	1347
LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)	1348
LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)	1354
Mandatos LOCK	1355
LOCK ADMIN (bloquear un administrador)	1355
LOCK NODE (Bloquear un nodo cliente)	1356
LOCK PROFILE (bloquear un perfil)	1357
MACRO (Invocar una macro)	1358
MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)	1359
Mandatos MOVE	1361
MOVE CONTAINER (Mover un contenedor)	1361
MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)	1363
MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)	1366
MOVE GRPMEMBER (Mover un miembro de grupo de servidores)	1378
MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)	1379
MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)	1385
Espacios de archivos para uno o más nodos o un grupo de proximidad	1386
Espacios de archivos seleccionados de un único nodo	1389
NOTIFY SUBSCRIBERS (Notificar a servidores gestionados que actualicen los perfiles)	1392
PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca)	1393
PING SERVER (Comprobar la conexión entre servidores)	1396
PREPARE (crear un archivo de plan de recuperación)	1397
PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)	1403
Mandatos QUERY	1408
QUERY ACTLOG (Consultar las anotaciones de actividades)	1409
QUERY ADMIN (Visualizar información de administrador)	1414
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	1418
QUERY ALERTSTATUS (Consultar el estado de una alerta)	1419
QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)	1423
QUERY AUDITOCCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)	1424
QUERY BACKUPSET (Consultar un juego de copias de seguridad)	1426
QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)	1430
QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)	1431
QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)	1433
QUERY COLLOGROUP (Consultar un grupo de proximidad)	1435
QUERY CONTAINER (Visualización de información de contenedor)	1437
QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)	1440
QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)	1446
QUERY COPYGROUP (Consultar grupos de copia)	1447
QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de nubes)	1451
QUERY DATAMOVER (visualizar definiciones de un transportador de datos)	1454
QUERY DB (Visualizar información de base de datos)	1456
QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)	1458
QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)	1459
QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)	1464
QUERY DIRSPACE (Consultar utilización de almacenamiento de directorios FILE)	1468
QUERY DOMAIN (Consultar un dominio de políticas)	1469
QUERY DRIVE (Consultar información acerca de una unidad)	1471
QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)	1474

QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)	1482
QUERY ENABLED (Consultar eventos activados)	1484
QUERY EVENT (Consultar eventos planificados y realizados)	1485
QUERY EVENT (Visualizar planificaciones de cliente)	1486
QUERY EVENT (Visualizar planificaciones de eventos de administración)	1491
QUERY EVENTRULES (Consultar reglas para eventos de servidor o de cliente)	1495
QUERY EVENTSERVER (Consultar el servidor de eventos)	1496
QUERY EXPORT (Consultar las operaciones de exportación activas o suspendidas)	1497
QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)	1502
QUERY FILESPACE (Consultar uno o más espacios de archivos)	1503
QUERY LIBRARY (Consultar una biblioteca)	1508
QUERY LIBVOLUME (Consultar un volumen de biblioteca)	1511
QUERY LICENSE (Visualizar información sobre licencias)	1513
QUERY LOG (Visualizar información sobre el registro de recuperación)	1515
QUERY MACHINE (Consultar información de máquina)	1517
QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)	1520
QUERY MGMTCLASS (Consultar una clase de gestión)	1525
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	1527
QUERY MONITORSTATUS (Consultar el estado de supervisión)	1529
QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)	1533
QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)	1534
QUERY NODE (Consultar nodos)	1538
QUERY NODEDATA (Consultar datos de cliente en volúmenes)	1546
QUERY NODEGROUP (Consultar un grupo de nodos)	1549
QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)	1550
QUERY OPTION (Consultar opciones del servidor)	1553
QUERY PATH (visualizar una definición de ruta)	1554
QUERY POLICYSET (Consultar un juego de políticas)	1558
QUERY PROCESS (Consultar uno o más procesos de servidor)	1559
QUERY PROFILE (Consultar un perfil)	1564
QUERY PROTECTSTATUS (Consultar estado de protección de una agrupación de almacenamiento)	1566
QUERY PROXYNODE (Consulta la autorización de proxy de un nodo cliente)	1568
QUERY PVUESTIMATE (Mostrar la estimación de unidades de valor de procesador)	1569
QUERY RECOVERYMEDIA (Consultar medio de recuperación)	1572
QUERY REPLICATION (Consultar los procesos de réplica de nodos)	1574
QUERY REPLNODE (Mostrar información sobre el estado de réplica de un nodo de cliente)	1582
QUERY REPLRULE (Consultar reglas de réplica)	1585
QUERY REPLSERVER (Consultar un servidor de réplica)	1586
QUERY REQUEST (Consultar una o más peticiones de montaje pendientes)	1588
QUERY RESTORE (Consultar sesiones de restauración reiniciables)	1589
QUERY RPFCONTENT (Consultar el contenido del archivo del plan de recuperación almacenado en un servidor de destino)	1591
QUERY RPFFILE (Consultar la información del archivo del plan de recuperación almacenado en un servidor de destino)	1592
QUERY SAN (Consultar los dispositivos de la SAN)	1594
QUERY SCHEDULE (Consultar planificaciones)	1596
QUERY SCHEDULE (Consultar planificaciones de cliente)	1597
QUERY SCHEDULE (Consultar una planificación de administración)	1600
QUERY SCRATCHPADENTRY (Consultar una entrada de registro)	1602
QUERY SCRIPT (Consultar scripts IBM Spectrum Protect)	1603
QUERY SERVER (Consultar un servidor)	1606
QUERY SERVERGROUP (Consultar un grupo de servidores)	1609
QUERY SESSION (Consultar sesiones de cliente)	1610
QUERY SHREDSTATUS (Consultar estado de destrucción)	1613
QUERY SPACETRIGGER (Consultar los desencadenantes de espacio)	1615
QUERY STATUS (Consultar parámetros del sistema)	1616
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	1625
QUERY STGPOOL (Consultar agrupaciones de almacenamiento)	1627
QUERY STGPOOLDIRECTORY (Consulta de un directorio de agrupaciones de almacenamiento)	1641
QUERY STGRULE (Visualizar información de reglas de almacenamiento)	1644

QUERY SUBSCRIBER (Visualizar información de suscriptor)	1646
QUERY SUBSCRIPTION (Visualizar información de inscripción)	1647
QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)	1648
QUERY TAPEALERTMSG (Visualizar estado del mandato SET TAPEALERTMSG)	1649
QUERY TOC (Visualizar tabla de contenido para una imagen de copia de seguridad)	1650
QUERY VIRTUALFSMAPPING (Consultar una correlación de espacios de archivos virtuales)	1652
QUERY VOLHISTORY (Visualizar información histórica de volúmenes secuenciales)	1653
QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)	1659
QUIT (finalizar la modalidad interactiva del cliente de administración)	1666
RECLAIM STGPOOL (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)	1666
RECONCILE VOLUMES (Reconciliar diferencias en definiciones de volúmenes virtuales)	1668
Mandatos REGISTER	1670
REGISTER ADMIN (Registrar un ID de administrador)	1670
REGISTER LICENSE (Registrar una nueva licencia)	1674
REGISTER NODE (Inscribir un nodo)	1675
Mandatos REMOVE	1689
REMOVE ADMIN (Suprimir un ID de usuario administrador)	1689
REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)	1690
REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)	1691
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	1693
REMOVE REPLSERVER (Eliminar un servidor de réplica)	1694
Mandatos RENAME	1695
RENAME ADMIN (redenominar un administrador)	1695
RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)	1696
RENAME NODE (Cambiar el nombre de un nodo)	1698
RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)	1700
RENAME SERVERGROUP (Redenominar un grupo de servidores)	1700
RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)	1701
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)	1702
REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)	1704
REPLY (Permitir una petición para continuar el proceso)	1712
RESET PASSEXP (restablecer caducidad de contraseña)	1712
RESTART EXPORT (Reiniciar una operación de exportación suspendida)	1713
Mandatos RESTORE	1714
RESTORE NODE (Restaurar un nodo NAS)	1714
RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)	1718
RESTORE VOLUME (Restaurar datos de volumen primario desde una agrupación de copia o agrupación de datos activos)	1721
Mandatos REVOKE	1725
REVOKE AUTHORITY (revocar autorización de administrador)	1725
REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)	1727
ROLLBACK (Retrotraer cambios no validados en una macro)	1728
RUN (ejecutar un script de IBM Spectrum Protect)	1729
SELECT (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)	1731
Mandatos SET	1739
SET ACCOUNTING (activar o desactivar registros de contabilidad)	1740
SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)	1741
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	1742
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	1743
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	1743
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	1744
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	1745
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	1746
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	1746
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	1747
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	1748
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	1749

SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)	1750
SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)	1751
SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)	1752
SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)	1753
SET CONFIGMANAGER (Especificar un gestor de configuración)	1754
SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)	1755
SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)	1756
SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)	1756
SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)	1757
SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)	1758
SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)	1760
SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)	1761
SET DEPLOYPKGGR (Habilitar el gestor de paquetes de despliegue)	1762
SET DEPLOYREPOSITORY (Establece la vía de acceso de descarga para los paquetes de despliegue del cliente)	1762
SET DEPLOYMAXPKGS (Establecer el número máximo de paquetes de despliegue del cliente para almacenar)	1763
DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)	1764
SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)	1765
SET DRMCHECKLABEL (Especificar comprobación de etiquetas)	1766
SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener mandatos)	1766
SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)	1767
SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)	1768
SET DRMCOURIERNAME (Especificar el nombre del transportista)	1769
SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)	1770
SET DRMFILEPROCESS (Especificar el proceso de archivos)	1771
SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)	1771
SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)	1773
SET DRMPPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)	1774
SET DRMPPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)	1776
SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)	1777
SET DRMRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)	1777
SET DRMVAULTNAME (Especificar el nombre de la cámara de seguridad)	1778
SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)	1779
SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)	1780
SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)	1781
SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)	1782
SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)	1782
SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)	1783
SET MAXCMDRETRIES (Establecer el número máximo de reintentos de mandato)	1784
SET MAXSCHEDULESESSIONS (Establecer número máximo de sesiones planificadas)	1785
SET MINPWLENGTH (Establecer longitud mínima de contraseña)	1785
SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)	1786
SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)	1787
SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)	1788
SET PASSEXP (Establecer fecha de caducidad de contraseña)	1789
SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)	1790
SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)	1792
SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)	1793
SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)	1794
SET REPLRETENTION (Establecer el período de retención de los registros de réplica)	1795
SET REPLSERVER (Establecer el servidor de réplica de destino)	1796
SET RETRYPERIOD (Establecer período de tiempo entre reintentos)	1797
SET SCHEDMODES (seleccionar modalidad de planificación central)	1798
SET SCRATCHPADRETENTION (Establecer hora de retención de registro)	1799
SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)	1799
SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)	1800
SET SERVERNAME (Especificar el nombre del servidor)	1801

SET SERVERPASSWORD (Establecer contraseña de servidor)	1801
SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)	1802
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	1803
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	1804
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	1805
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	1807
SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)	1808
SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)	1809
SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)	1809
SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)	1810
SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)	1811
SETOPT (Establecer una opción de servidor para actualización dinámica)	1812
SHRED DATA (destruir datos)	1813
SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)	1815
Mandatos UNLOCK	1816
UNLOCK ADMIN (Desbloquear un administrador)	1816
UNLOCK NODE (Desbloquear un nodo cliente)	1817
UNLOCK PROFILE (Desbloquear un perfil)	1818
Mandatos UPDATE	1818
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	1819
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	1821
UPDATE ADMIN (Actualizar un administrador)	1822
UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)	1826
UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)	1829
UPDATE CLOPTSET (Actualizar la descripción de un conjunto de opciones de cliente)	1830
UPDATE COLLOGGROUP (Actualizar un grupo de proximidad)	1831
UPDATE COPYGROUP (Actualizar un grupo de copia)	1832
UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)	1832
UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)	1836
UPDATE DATAMOVER (Actualizar un transportador de datos)	1837
UPDATE DEVCLASS (Actualizar los atributos de una clase de dispositivo)	1839
3590	1839
3592	1842
4MM	1847
8MM	1850
Centera	1854
DLT	1856
Ecartridge	1859
Archivo	1864
Generictape	1868
LTO	1869
NAS	1874
Removablefile	1876
Servidor	1877
VolSafe	1878
UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS)	1881
3590, para el servidor de medios de z/OS	1882
3592, para el servidor de medios de z/OS	1885
ECARTRIDGE, para el servidor de medios de z/OS	1889
FILE, para el servidor de medios de z/OS	1892
UPDATE DOMAIN (Actualizar un dominio de políticas)	1894
UPDATE DRIVE (Actualizar una unidad)	1896
UPDATE FILESPACE (Actualizar reglas de réplica de nodos de espacio de archivos)	1899
UPDATE LIBRARY (Actualizar una biblioteca)	1903
349X	1904
ACSLs	1906
EXTERNAL	1907

FILE	1908
MANUAL	1909
SCSI	1910
Compartido	1912
VTL	1913
UPDATE LIBVOLUME (Cambiar el estado de un volumen de almacenamiento)	1915
UPDATE MACHINE (Actualizar información de máquina)	1916
UPDATE MGMTCLASS (Actualizar una clase de gestión)	1917
UPDATE NODE (Actualizar atributos del nodo)	1919
UPDATE NODEGROUP (Actualizar un grupo de nodos)	1933
UPDATE PATH (cambiar una ruta)	1934
El destino es una unidad	1935
El destino es una biblioteca	1939
El destino es una biblioteca ZOSMEDIA	1941
UPDATE POLICYSET (Actualizar la descripción de un juego de políticas)	1941
UPDATE PROFILE (Actualizar una descripción de perfil)	1942
UPDATE RECOVERYMEDIA (Actualizar medio de recuperación)	1943
UPDATE REPLRULE (Actualizar reglas de réplica)	1944
UPDATE SCHEDULE (Actualizar una planificación)	1945
UPDATE SCHEDULE (Actualizar una planificación de cliente)	1946
UPDATE SCHEDULE (Actualizar una planificación de administración)	1956
UPDATE SCRATCHPADENTRY (Actualizar una entrada de registro)	1962
UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)	1963
UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)	1965
UPDATE SERVERGROUP (Actualizar una descripción de grupo de servidores)	1969
UPDATE SPACETRIGGER (Actualizar los desencadenantes de espacio)	1970
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	1972
UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)	1975
Agrupación de almacenamiento de contenedores en la nube	1976
Agrupación de almacenamiento de contenedores de directorio	1979
Agrupación de almacenamiento de copia de contenedor	1983
Agrupación de acceso aleatorio primaria	1985
Agrupación de acceso secuencial primaria	1993
Agrupación de copias	2004
Agrupación de datos activos	2009
UPDATE STGPOOLDIRECTORY (Actualización de un directorio de agrupaciones de almacenamiento)	2014
UPDATE STGRULE (Actualizar una regla de almacenamiento para uno o más agrupaciones de almacenamiento)	2016
UPDATE VIRTUALFSMAPPING (Actualizar una correlación de espacios de archivos virtuales)	2018
UPDATE VOLHISTORY (Actualizar información histórica de volúmenes secuenciales)	2019
UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)	2021
Mandatos VALIDATE	2024
VALIDATE ASPERA (Validación de una configuración Aspera FASP)	2024
VALIDATE CLOUD (Validar credenciales de nube)	2027
VALIDATE LANFREE (Validar rutas fuera de la LAN)	2029
VALIDATE POLICYSET (Verificar un juego de políticas)	2030
VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)	2031
VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)	2034
VARY (Activar o desactivar un volumen de acceso aleatorio)	2036
Opciones de servidor	2037
Modificación de opciones del servidor	2045
Tipos de opciones del servidor	2045
Opciones de comunicación del servidor	2046
Opciones de almacenamiento del servidor	2047
Opciones de cliente/servidor	2049
Opciones de fecha, número, hora e idioma	2049
Opciones de la base de datos	2049
Opciones de transferencia de datos	2050
Opciones de mensajes	2050

Opciones de anotaciones de eventos	2050
Opciones de seguridad y del sistema de licencias	2051
Opciones varias	2052
3494SHARED	2052
ACSACCESSID	2053
ACSLOCKDRIVE	2053
ACSQUICKINIT	2053
ACSTIMEOUTX	2054
ACTIVELOGDIRECTORY	2054
ACTIVELOGSIZE	2055
ADMINCOMMTIMEOUT	2055
ADMINIDLETIMEOUT	2056
ADMINONCLIENTPORT	2056
ADSMGROUPNAME	2057
ALIASHALT	2057
ALLOWDESAUTH	2057
ALLOWREORGINDEX	2058
ALLOWREORGTABLE	2058
ARCHFAILOVERLOGDIRECTORY	2059
ARCHLOGCOMPRESS	2059
ARCHLOGDIRECTORY	2060
ARCHLOGUSEDTHRESHOLD	2060
ASSISTVCRRECOVERY	2061
AUDITSTORAGE	2061
BACKUPINITIATIONROOT	2062
CHECKTAPEPOS	2062
CLIENTDEDUPTXNLIMIT	2063
CLIENTDEPLOYCATALOGURL	2064
CLIENTDEPLOYUSELOCALCATALOG	2064
COMMMETHOD	2065
COMMTIMEOUT	2066
CONTAINERRESOURCESTIMEOUT	2066
DATEFORMAT	2067
DBDIAGLOGSIZE	2067
DBDIAGPATHFSTHRESHOLD	2068
DBMEMPERCENT	2069
DBMTCPPORT	2069
DEDUPREQUIRESBACKUP	2070
DEDUPTIER2FILESIZE	2070
DEDUPTIER3FILESIZE	2071
DEVCONFIG	2071
DISABLEREORGTABLE	2072
DISABLESCHEDS	2072
DISPLAYLFINFO	2073
DNSLOOKUP	2074
DRIVEACQUIRERETRY	2074
ENABLENASDEDUP	2074
EVENTSERVER	2075
EXPINTERVAL	2075
EXPQUIET	2076
FASPBEGPORT	2076
FASPENDPORT	2077
FASPTARGETRATE	2077
FFDCLOGLEVEL	2078
FFDCLOGNAME	2079
FFDCMAXLOGSIZE	2079
FFDCNUMLOGS	2080
FILEEXIT	2080

FILETEXTEXIT	2081
FSUSEDTHRESHOLD	2081
IDLETIMEOUT	2082
KEEPALIVE	2082
KEEPALIVETIME	2083
KEEPALIVEINTERVAL	2083
LANGUAGE	2084
LDAPCACHEDURATION	2086
LDAPURL	2087
MAXSESSIONS	2087
MESSAGEFORMAT	2088
MIRRORLOGDIRECTORY	2088
MOVEBATCHSIZE	2089
MOVESIZETHRESH	2089
MSGINTERVAL	2089
NAMEDPIPENAME	2090
NDMPCONNECTIONTIMEOUT	2090
NDMPCONTROLPORT	2090
NDMPENABLEKEEPALIVE	2091
NDMPKEEPIDLEMINUTES	2091
NDMPPORTRANGE	2092
NDMPPREFDATAINTERFACE	2092
NOPREEMPT	2093
NORETRIEVEDATE	2093
NPAUDITFAILURE	2094
NPAUDITSUCCESS	2094
NPBUFFERSIZE	2095
NUMBERFORMAT	2095
NUMOPENVOLSALLOWED	2096
PUSHSTATUS	2097
QUERYAUTH	2097
RECLAIMDELAY	2098
RECLAIMPERIOD	2098
REORGBEGINTIME	2099
REORGDURATION	2099
REPORTRETRIEVE	2100
REPLBATCHSIZE	2100
REPLSIZETHRESH	2101
REQSYSAUTHOUTFILE	2101
RESOURCETIMEOUT	2102
RESTHTTPSPORT	2102
RESTOREINTERVAL	2103
RETENTIONEXTENSION	2103
SANDISCOVERY	2104
SANDISCOVERYTIMEOUT	2104
SANREFRESHTIME	2105
SEARCHMPQUEUE	2105
SECUREPIPES	2106
SERVERDEDUPTXNLIMIT	2106
SHMPORT	2107
SHREDDING	2107
SNMPHEARTBEATINTERVAL	2108
SNMPMESSAGECATEGORY	2108
SNMPSUBAGENT	2109
SNMPSUBAGENTHOST	2109
SNMPSUBAGENTPORT	2110
SSLFIPSMODE	2110
SSLINITTIMEOUT	2110

SSLTCPADMINPORT	2111
SSLTCPPOINT	2111
TCPADMINPORT	2112
TCPBUFSIZE	2113
TCPNODELAY	2113
TCPPOINT	2114
TCPWINDOWSIZE	2114
TECBEGINEVENTLOGGING	2115
TECHOST	2115
TECPOINT	2116
TECUTF8EVENT	2116
THROUGHPUTDATATHRESHOLD	2116
THROUGHPUTTIMETHRESHOLD	2117
TIMEFORMAT	2117
TXNGROUPMAX	2118
UNIQUEDPTECEVENTS	2119
UNIQUECEVENTS	2119
USEREXIT	2119
VERBCHECK	2120
VOLUMEHISTORY	2121
Herramientas del servidor	2121
DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)	2122
DSMSERV (Iniciar el servidor)	2123
Script de inicio del servidor: rc.dsmserv	2124
Script de inicio del servidor: dsmserv.rc	2125
DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)	2126
DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)	2127
DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)	2128
DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)	2130
DSMSERV INSERTDB (Mover una base de datos de servidor a una base de datos vacía)	2132
DSMSERV LOADFORMAT (Formatear una base de datos)	2134
DSMSERV REMOVEDB (Eliminar una base de datos)	2136
DSMSERV RESTORE DB (Restaurar la base de datos)	2137
DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)	2137
DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)	2140
DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)	2143
DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)	2144
Programas de utilidad de dispositivo	2145
AIX: tsmdlst (Visualizar información sobre dispositivos)	2145
Linux: autoconf (dispositivos de configuración automática)	2145
Windows: tsmdlst (Visualizar información sobre dispositivos)	2147
Scripts de servidor y macros para automatización	2149
Scripts de servidor	2149
Definición de un script de servidor	2150
Ejecución de mandatos en paralelo o en serie	2150
Continuación de mandatos a través de varias líneas de mandatos	2151
Inclusión de las variables de sustitución en un script	2152
Inclusión de sentencias de flujo lógico en un script	2152
Especificación de la cláusula IF	2152
Especificación de la sentencia EXIT	2153
Especificación de la sentencia GOTO	2153
Utilización de mandatos SELECT en un script	2153
Actualización de un script	2154
Añadir un nuevo mandato	2154
Sustitución de un mandato existente	2155
Adición de un mandato y un número de línea	2155
Supresión de un mandato de un script del servidor	2155
Consulta de un script de servidor para crear otro script de servidor	2156

Ejecución de un script del servidor	2156
Macros de cliente administrativo	2156
Grabación de mandatos en una macro	2157
Grabación de comentarios en una macro	2157
Inclusión de caracteres de continuación en una macro	2158
Inclusión de las variables de sustitución en un macro	2158
Ejecución de una macro	2159
Proceso de mandatos en una macro	2159
Códigos de retorno de los scripts para IBM Spectrum Protect	2160
Archivos PDF	2162
Clientes	2162
API	2163
Rendimiento	2163
Resolución de problemas	2163
Mensajes, códigos de retorno y códigos de error	2163
Introducción a los mensajes	2163
Formato de los mensajes de cliente y servidor de IBM Spectrum Protect	2164
Interpretación de los mensajes de código de retorno	2165
Ejemplo uno para el mandato QUERY EVENT	2166
Ejemplo dos para el mandato DEFINE VOLUME	2166
Mensajes de ANE	2167
Mensajes de ANR	2167
Mensajes ANS 0000-9999	2167
Códigos de retorno de API	2168
Descripciones de código de E/S en mensajes del servidor	2168
Visión general de descripciones de los códigos de terminación y de operación de controladores de dispositivos	2169
Valores del código de terminación comunes a todas las clases de dispositivos	2169
Valores del código de terminación para cambiadores de medios	2170
Valores de código de finalización para controladores de cinta	2172
Descripciones de códigos de ASC y ASCQ estándares	2173
Códigos de error de dispositivo en el registro de errores del sistema AIX	2176
Códigos de retorno de IBM Global Security Kit	2177
Glosario	2187
A	2187
B	2191
C	2191
D	2194
E	2194
F	2195
G	2195
H	2196
I	2197
J	2197
K	2197
L	2197
M	2198
N	2199
O	2200
P	2200
Q	2201

R	2201
S	2203
T	2205
U	2205
V	2206
W	2206

Documentación de IBM Spectrum Protect

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

Cómo empezar

- Instalación y actualización de servidores
- Instalación y actualización del Centro de operaciones
- Selección e implementación de soluciones de protección de datos
- Novedades en el servidor
- [🔗 Vídeos de novedades](#)
- Archivos PDF


Tareas comunes

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

Resolución de problemas y ayuda

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

Más información

-  Sugerencias de usuario para IBM® Knowledge Center
- Suites de producto y productos relacionados
- [🔗](#) Página de inicio de la familia de productos
- [🔗](#) Wiki de productos IBM Spectrum Protect
- [🔗](#) IBM Spectrum Protect Developer Center
- [🔗](#) Publicaciones de IBM Redbooks
- [🔗](#) IBM Skills Gateway for Systems
- Accesibilidad
- Avisos legales del producto

© Copyright IBM Corp. 1993, 2017

Funciones de accesibilidad para la familia de productos IBM Spectrum Protect

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

Visión general

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

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

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

release más reciente del lector de pantalla y el navegador web más reciente soportados por el producto.

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

Navegación con el teclado

Este producto utiliza teclas estándar de navegación.

Información sobre interfaces

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

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

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

Software del proveedor

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

Información de accesibilidad relacionada

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

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

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

Suites de producto y productos relacionados

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

Suites de producto y opciones de licencia

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

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

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

Productos relacionados

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

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

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

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

Archivos PDF

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

Archivos PDF precompilados

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

- Soluciones de protección de datos
- Servidores

Paquete de archivos PDF

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

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

Actualizaciones en este release

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

Componente	Resumen de las actualizaciones	Notas del release de V8.1
Componentes de servidor	Actualizaciones	Notas de release

Conceptos de IBM Spectrum Protect

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

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

Visión general de IBM Spectrum Protect

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

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

Componentes de protección de datos

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

Servidor

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

El inventario incluye los siguientes componentes:

Base de datos

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

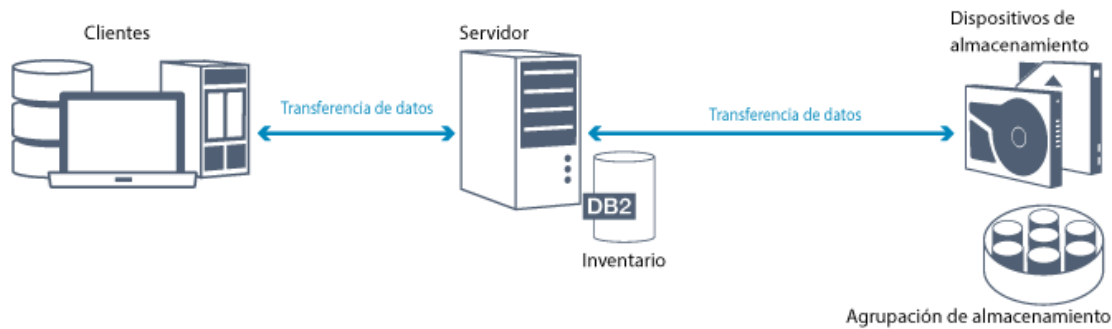
Registro de recuperación

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

Sistemas y aplicaciones cliente

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

Figura 1. Componentes de la solución de protección de datos



Software de cliente

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

Nodos de cliente

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

Soportes de almacenamiento

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

Dispositivos de almacenamiento

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

Agrupaciones de almacenamiento

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

Servicios de protección de datos

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

Tipos de servicios de protección de datos

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

Figura 1. Servicios de protección de datos



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

Copia de seguridad y restauración de servicios

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

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

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

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

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

Servicios de archivado y recuperación

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

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

El servicio de recuperación proporciona las siguientes funciones:

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

Migrar y recuperar servicios

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

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

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

Tipos de datos de cliente que se pueden proteger

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

Clientes de aplicaciones

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

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

Máquinas virtuales

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

Clientes de sistema

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

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

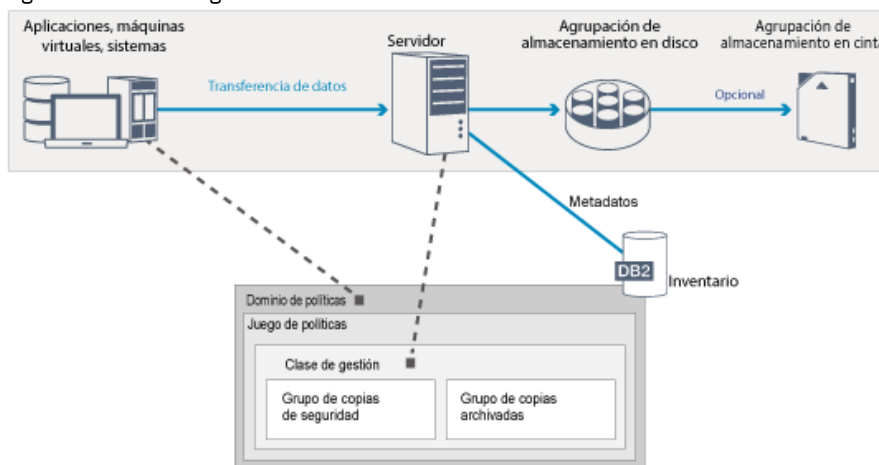
Procesos para gestionar la protección de datos con IBM Spectrum Protect

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

Proceso de gestión de datos

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

Figura 1. Proceso de gestión de datos



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

Componentes de inventario

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

Base de datos del servidor

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

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

Registro de recuperación

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

Registro activo

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

Duplicación de anotaciones (opcional)

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

Registro de archivos

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

Anotaciones de recuperación de errores de archivado (opcional)

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

Gestión de datos basada en políticas

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

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

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

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

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

Cree políticas definiendo los siguientes componentes de política:

Dominio de políticas

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

Juego de políticas

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

Clase de gestión

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

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

Grupo de copias

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

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

Gestión de la seguridad

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

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

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

Inscripción abierta

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

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

Inscripción cerrada

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

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

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

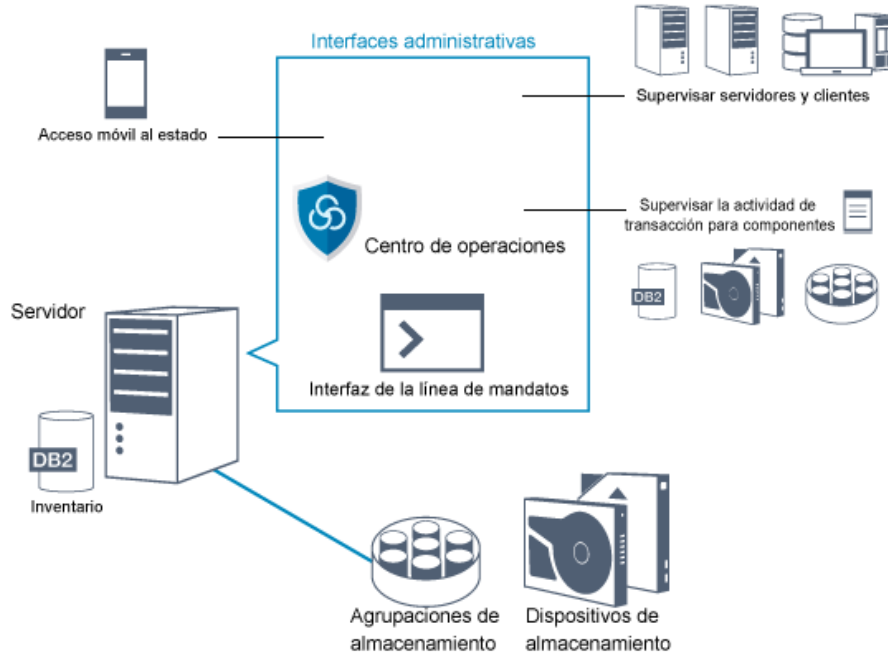
Interfaces de usuario para entornos de IBM Spectrum Protect

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

Interfaces para la gestión de almacenamiento de datos

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

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



Utilice las interfaces siguientes para interactuar con IBM Spectrum Protect:

Centro de operaciones

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

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

Interfaz de la línea de mandatos

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

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

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

Interfaces para la gestión de actividad de cliente

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

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

Conceptos de almacenamiento de datos en IBM Spectrum Protect

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

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

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

Tipos de dispositivos de almacenamiento

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

Dispositivos de almacenamiento y objetos de almacenamiento

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

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

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

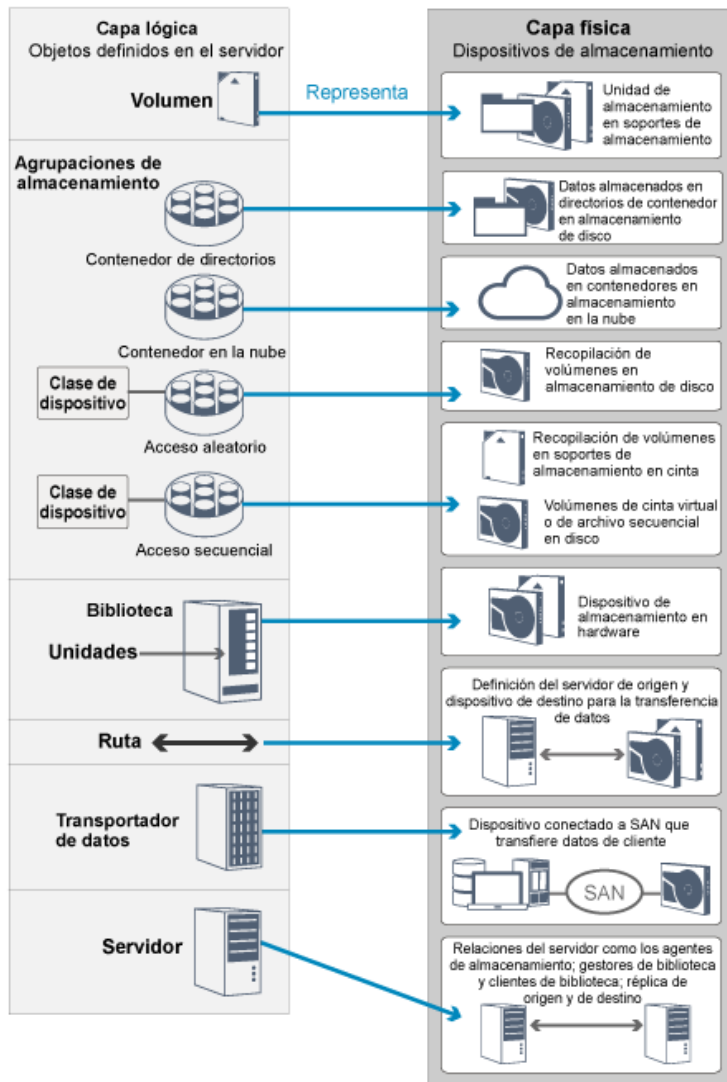
Tabla 1. Objetos de almacenamiento y representaciones

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

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

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

Figura 1. Objetos de almacenamiento



Dispositivos de disco

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

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

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

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

Dispositivos de cinta física

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

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

El traslado de datos a cinta proporciona los siguientes beneficios:

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

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

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

Bibliotecas virtuales de cintas

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

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

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

Almacenamiento de datos en agrupaciones de almacenamiento

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

Tipos de agrupaciones de almacenamiento

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

Agrupaciones de almacenamiento primarias

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

Agrupaciones de almacenamiento de copia

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

Agrupaciones de almacenamiento de copia de contenedor

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

Agrupaciones de almacenamiento de datos activos

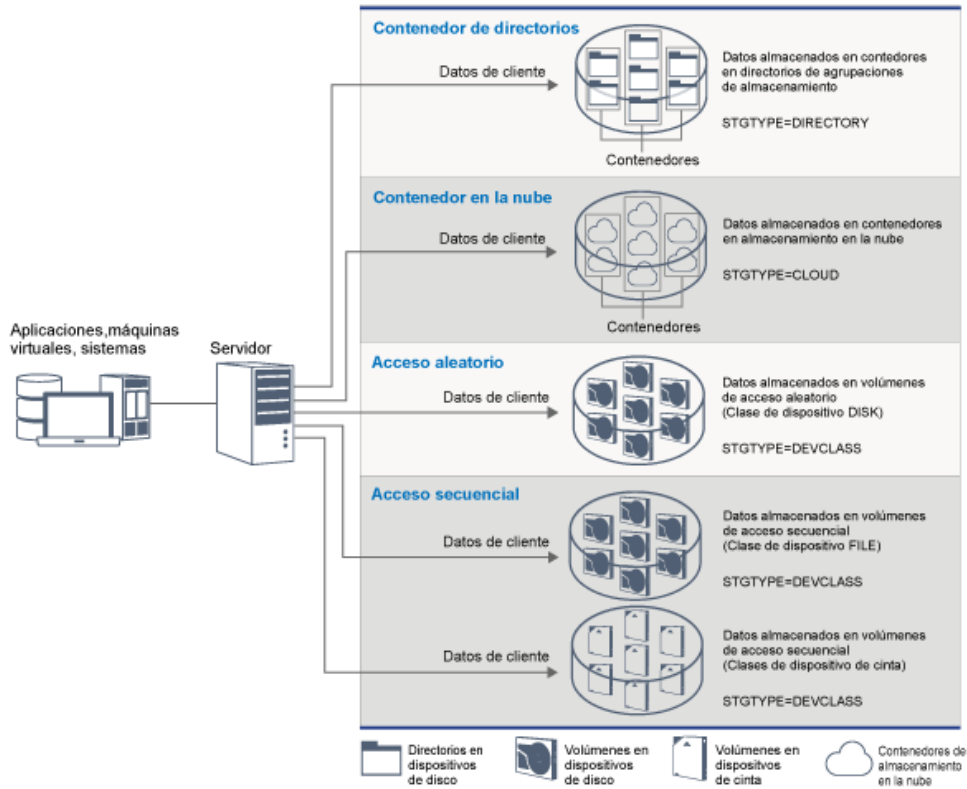
Conjunto denominado de volúmenes de agrupación de almacenamiento que solamente contiene versiones activas de datos de copia de seguridad de cliente.

Agrupaciones de almacenamiento primarias

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

Figura 1. Agrupaciones de almacenamiento primarias

Agrupaciones de almacenamiento primario



Puede definir los siguientes tipos de agrupación de almacenamiento primario:

Agrupaciones de almacenamiento de contenedores de directorio

Una agrupación de almacenamiento que el servidor utiliza para almacenar datos en contenedores en directorios de agrupación de almacenamiento. Los datos que se almacenan en una agrupación de almacenamiento de contenedores de directorios pueden utilizar deduplicación de datos en línea, deduplicación de datos del lado del cliente, compresión en línea o compresión del lado del cliente. La deduplicación de datos en línea o la compresión en línea reduce los datos a la vez que se almacenan. Consejo: Los datos que se comprimen primero no podrán deduplicarse, no obstante, los datos deduplicados pueden comprimirse.

Al utilizar agrupaciones de almacenamiento de contenedores de directorio, elimina la necesidad de reclamación de volumen, que mejora el rendimiento de servidor y reduce el coste del hardware de almacenamiento. Puede proteger y reparar los datos de las agrupaciones de almacenamiento de contenedores de directorio a nivel de la agrupación de almacenamiento. Puede nivelar datos que estén almacenados en una agrupación de almacenamiento de contenedor de directorios en una agrupación de almacenamiento de contenedor en la nube.

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

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

Agrupaciones de almacenamiento de contenedores de nube

Una agrupación de almacenamiento que un servidor utiliza para almacenar datos en almacenamiento en nube. El almacenamiento en la nube puede estar en el local o fuera de este. Las agrupaciones de almacenamiento de contenedores de nube proporcionadas por IBM Spectrum Protect pueden almacenar datos en un almacenamiento en nube que esté basado en objetos. Mediante el almacenamiento de datos en agrupaciones de almacenamiento de contenedores de nube, puede aprovechar las ventajas de coste por unidad que ofrecen las nubes junto con las prestaciones de escalabilidad que proporciona el almacenamiento en nube. Puede utilizar la definición por niveles de la nube para reducir los costes de mover los datos de un almacenamiento en disco a una agrupación del almacenamiento en contenedor de nube. IBM Spectrum Protect gestiona las credenciales, la seguridad, las E/S de lectura y escritura y el ciclo de vida de los datos almacenados en la nube. Cuando se implementan agrupaciones de almacenamiento de contenedores de nube en el servidor, puede grabar directamente en la nube

configurando una agrupación de almacenamiento de contenedores de nube con las credenciales de la nube. Los datos que se almacenan en una agrupación de almacenamiento de contenedor en la nube utilizan la deduplicación de datos en línea y la compresión en línea. El servidor graba datos deduplicados y cifrados directamente en la nube. Puede hacer la copia de seguridad y la restauración de datos o archivar y recuperar datos directamente de la agrupación de almacenamiento de contenedores de nube.

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

En las instalaciones

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

Fuera de las instalaciones locales

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

Agrupaciones de almacenamiento asociadas con clases de dispositivo

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

Clase de dispositivo DISK

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

Clase de dispositivo FILE

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

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

ARCHIVEPOOL

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

BACKUPPOOL

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

SPACEMGPOOL

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

Agrupaciones de almacenamiento de copia

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

Figura 2. Agrupaciones de almacenamiento de copia



Las agrupaciones de almacenamiento de copia proporciona un medio de recuperación ante siniestro o anomalías de medios. Por ejemplo, si un cliente intenta recuperar un archivo dañado de la agrupación de almacenamiento primario y la agrupación de almacenamiento no está disponible o el archivo de la agrupación de almacenamiento está dañado, el cliente puede restaurar los datos de la agrupación de almacenamiento de copias.

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

Agrupaciones de almacenamiento de copia de contenedor

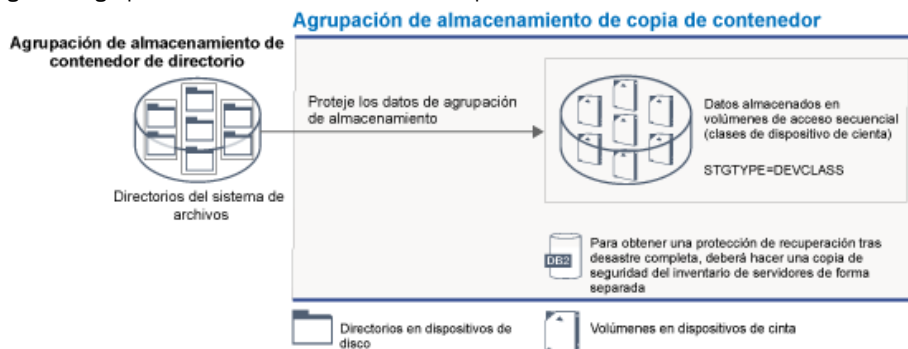
Un servidor puede proteger una agrupación de almacenamiento de contenedores de directorio almacenando copias de los datos en una agrupación de almacenamiento de copias de contenedor. Los datos en las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta, que se pueden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

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

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

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

Figura 3. Agrupaciones de almacenamiento de copia de contenedor



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

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

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

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

Agrupaciones de almacenamiento de datos activos

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

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

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

Figura 4. Agrupaciones de almacenamiento de datos activos



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

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

Información relacionada:

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

Transporte de datos a almacenar a través de redes

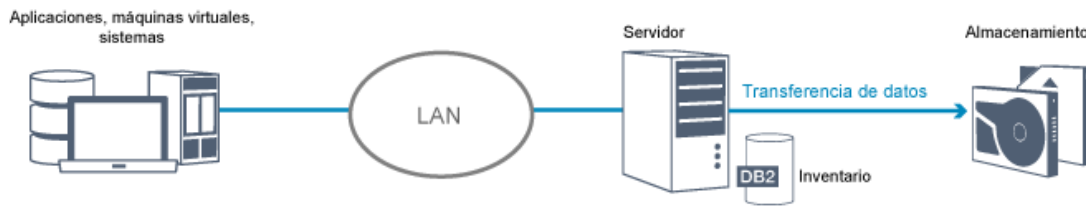
En entorno de IBM Spectrum Protect proporciona formas de mover datos de forma segura para almacenarlos a través de varios tipos de redes y configuraciones.

Configuraciones de red para dispositivos de almacenamiento

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

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

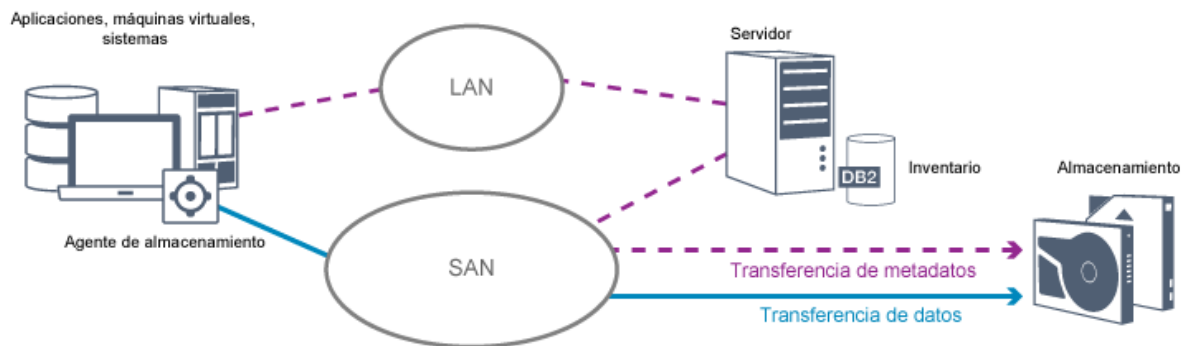
Figura 1 muestra la vía de acceso a datos para operaciones de copia de seguridad de IBM Spectrum Protect a través de una LAN. Figura 1. Operaciones de copia de seguridad de IBM Spectrum Protect a través de una LAN



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

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

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



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

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

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

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

Almacenamiento conectado a red

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

- IBM Spectrum Protect hace copia de seguridad de un servidor de archivos de NAS en un dispositivo de biblioteca adjunto directamente a un servidor de archivos de NAS. El servidor de archivos de NAS, que puede estar lejos del servidor IBM Spectrum Protect, transfiere directamente los datos de copia de seguridad a una unidad de una biblioteca de cintas con conexión SCSI. Los datos están almacenados en agrupaciones de almacenamiento con formato NDMP, de las que se puede hacer copia de seguridad en el soporte de almacenamiento que se pueden mover fuera del sitio como medida de protección en caso de que se produzca un desastre en el sitio.

- IBM Spectrum Protect hace una copia de seguridad de un servidor de archivos de almacenamiento adjunto de red (NAS) sobre la LAN en una jerarquía de agrupación de almacenamiento. En este tipo de configuración, puede almacenar datos de NAS directamente en el disco, ya sea acceso aleatorio o acceso secuencial y, a continuación, migrar los datos a cinta. También puede utilizar este tipo de configuración para la réplica del sistema. También se puede hacer copia de seguridad de los datos en un soporte de almacenamiento que se puede mover fuera del sitio. La ventaja de este tipo de configuración es que le aporta todas las características de gestión de datos asociadas a una jerarquía de agrupaciones de almacenamiento.
- El cliente de IBM Spectrum Protect lee los datos desde el sistema de NAS mediante los protocolos NFS o CIFS y los envía al servidor para almacenarlos.

Gestión de almacenamiento

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

Tipos de dispositivos para almacenamiento del servidor

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

Migración de datos a través de la jerarquía de almacenamiento

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

Eliminación de datos caducados

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

Reutilización de medios mediante reclamación

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

Consolidación de datos de cliente de seguridad

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

Colocación de datos de cliente

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

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

Asociación de agrupaciones de datos activos con varios dispositivos

Las agrupaciones de datos activos son útiles para la restauración rápida de datos de cliente. Los beneficios incluyen una reducción del número de volúmenes de almacenamiento en el sitio o fuera, o la reducción del ancho de banda al copiar o

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

Creación de un conjunto de copias de seguridad

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

Movimiento de datos para un nodo de cliente

Puede consolidar datos para un nodo cliente mediante el traspaso de datos dentro del almacenamiento del servidor. Puede mover un conjunto de copias de seguridad a un soporte diferente, donde el conjunto de copias de seguridad se retiene hasta la hora que especifica. Los datos consolidados puede ayudar a mejorar la eficiencia durante las operaciones de restauración o recuperación de clientes.

Estrategias de protección de datos con IBM Spectrum Protect

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

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

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

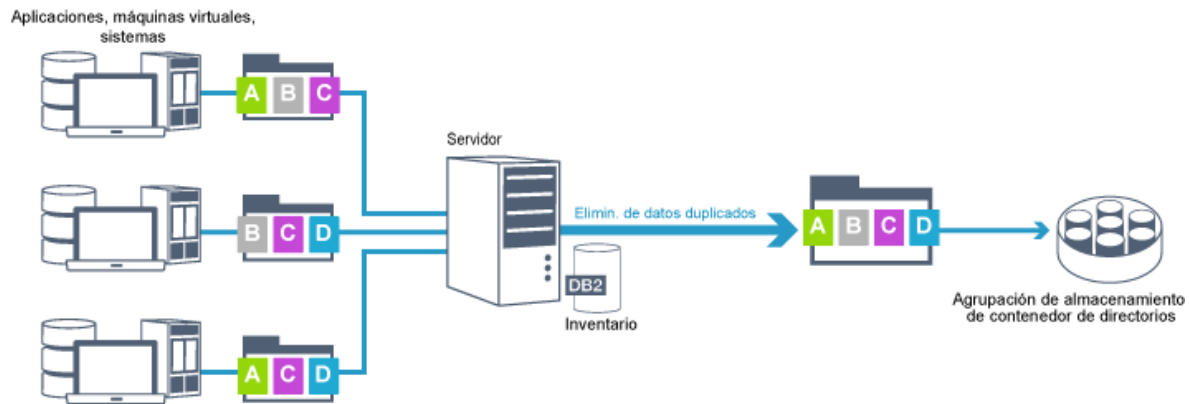
Estrategias para minimizar el uso del espacio de almacenamiento para copias de seguridad

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

Eliminación de datos duplicados

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

Figura 1. proceso de optimización de almacenamiento de datos



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

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

Eliminación de datos duplicados del lado del servidor

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

- Elimina la necesidad de reclamación
- Reduce el espacio ocupado por los datos almacenados

Eliminación de datos duplicados del lado del cliente

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

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

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

Compresión

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

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

Copia de seguridad incremental progresiva

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

Estrategias para protección ante desastres

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

Réplica a un sitio remoto

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

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

Ventajas

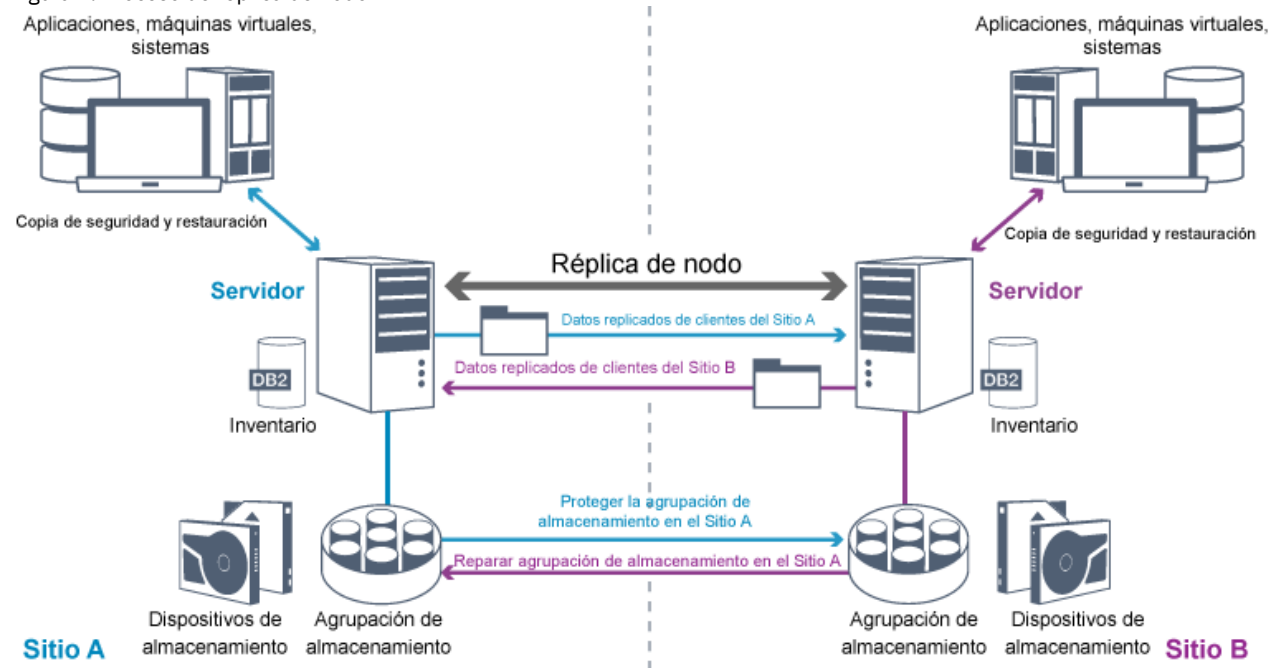
- Migración tras error para que los datos estén disponibles inmediatamente si se produce un desastre.
- Réplica incremental, que acelera la transmisión de datos.
- Transferencia electrónica
- Protege los datos y la mayoría de los metadatos

Inconvenientes

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

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

Figura 1. Proceso de réplica de nodo



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

IBM Spectrum Protect proporciona las siguientes funciones de réplica:

- Puede definir políticas respecto al servidor de destino de las siguientes formas:
 - Políticas idénticas en el servidor de origen y el servidor de destino
 - Políticas diferentes en el servidor de origen y el servidor de destino, que cumplen distintos requisitos empresariales.
- Si se produce un siniestro y el servidor de origen no está disponible, el cliente puede recuperar los datos del servidor de destino. Si no se puede recuperar el servidor de origen, puede dirigir a los clientes a almacenar datos en el servidor de destino. Cuando se produce una parada, los clientes con copias de seguridad en el servidor de origen pueden migrar automáticamente sus datos para restauración desde el servidor de destino.

- Puede utilizar el proceso de réplica para recuperar archivos dañados de las agrupaciones de almacenamiento. Debe replicar los datos de cliente para el servidor de destino antes de que se produzca un daño en el archivo. Los procesos de réplica posteriores detectan archivos dañados en el servidor de origen y los sustituyen por archivos no dañados del servidor de destino.

Rol de réplica en la protección ante desastres

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

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

Protección de agrupaciones de almacenamiento

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

Ventajas

- Recuperación rápida y reconstrucción del sistema de origen.

Inconvenientes

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

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

Agrupaciones de almacenamiento de contenedores de directorio

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

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

Agrupaciones de almacenamiento de copia de contenedor

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

Agrupaciones de almacenamiento asociadas con clases de dispositivo FILE y DISK

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

Copias de seguridad de bases de datos

Utilice las copias de seguridad de bases de datos para recuperar el sistema tras un daño en la base de datos. Además, se deben utilizar las operaciones de copia de seguridad de bases de datos para impedir que DB2 se quede sin espacio de registro de archivado. Las operaciones de copia de seguridad de bases de datos no forman parte de la réplica de nodo. Una copia de seguridad de base de datos puede ser completa, incremental o de instantánea. Para prepararse para la recuperación tras desastre, debe restaurarse una copia de

las copias de seguridad de la base de datos fuera del local. Para restaurar la base de datos, debe tener los volúmenes de copia de seguridad para la base de datos. La base de datos se puede restaurar desde volúmenes de copia de seguridad mediante una restauración a un momento específico o mediante una operación de restauración más actual.

Restauración a un instante específico

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

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

Restauración más actual

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

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

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

Métodos alternativos para la protección ante desastres

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

Enviando cintas de copia de seguridad a un sitio remoto

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

Réplica de dispositivo multisitio a un servidor en espera

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

Comparación de estrategias de configuración de protección

Considere los siguientes escenarios de pérdida de datos potencial:

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

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

Configuraciones solo para protección frente a daños

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

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

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

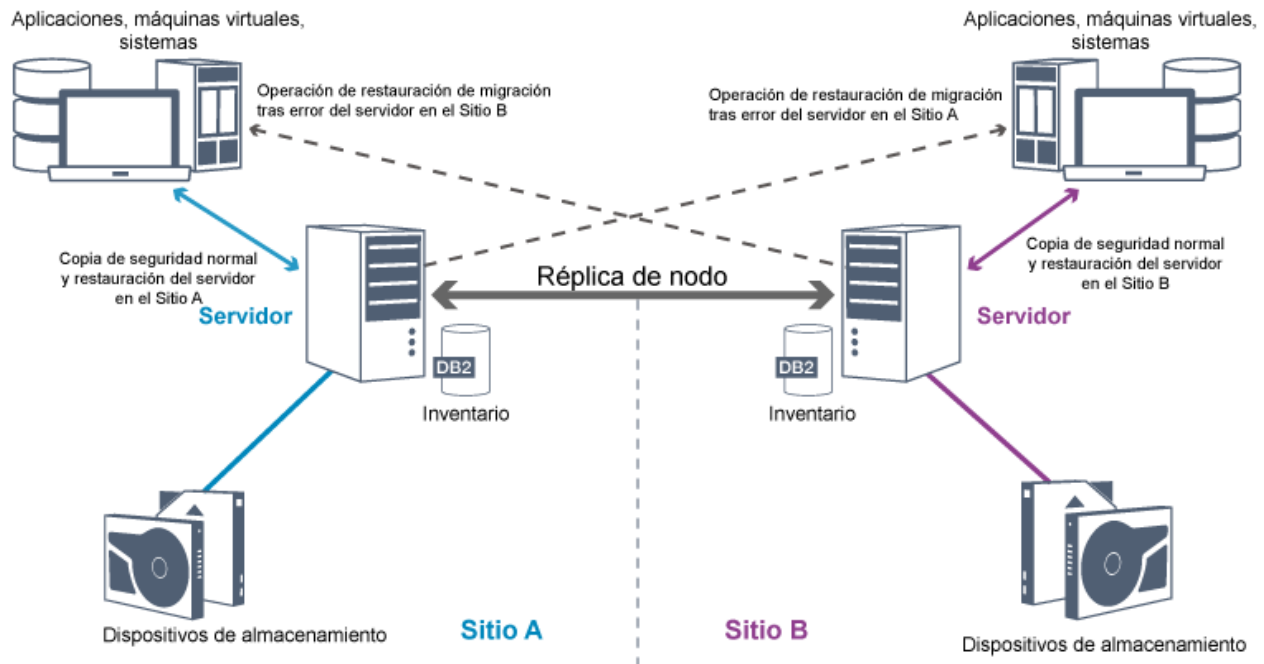
Estrategias para la recuperación tras desastre con IBM Spectrum Protect

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

Migración tras error automática para la recuperación tras desastre

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

Figura 1. Proceso de migración tras error automática



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

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

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

Recuperación de componentes de IBM Spectrum Protect

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

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

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

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

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

Medidas preventivas para la recuperación

La recuperación se basa en las siguientes medidas de precaución:

- Duplicación, mediante la cual el servidor mantiene una copia del registro activo
- Hacer una copia de seguridad de la base de datos.
- Copia de seguridad de las agrupaciones de almacenamiento
- Auditoría de las agrupaciones de almacenamiento de archivos dañados y la recuperación de archivos dañados según convenga
- Copia de seguridad de la configuración de dispositivos y de los archivos de historial de volumen
- Validación de los datos en agrupaciones de almacenamiento mediante la comprobación de redundancia cíclica
- Almacenamiento del archivo cert.kdb en un lugar seguro para garantizar que la capa de sockets seguros (SSL) está protegida

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

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

Soluciones de protección de datos de IBM Spectrum Protect

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

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

Selección de una solución de protección de datos para el entorno

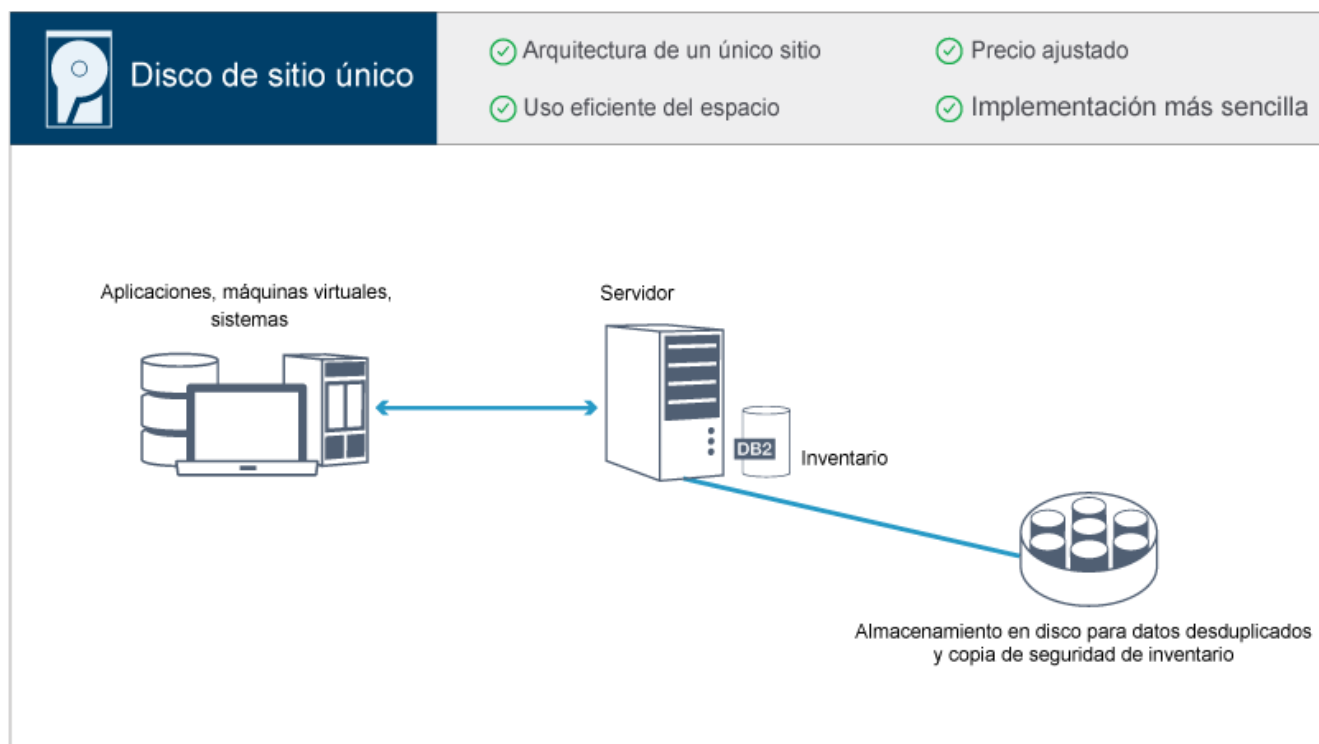
Para ayudarle a desplegar un entorno de protección de datos, revise la información sobre las configuraciones de IBM Spectrum Protect de uso recomendado y seleccione la mejor solución para las necesidades de negocio.

- Implementación basada en disco de una solución de protección de datos para un sitio único
Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea y proporciona protección para los datos en un único sitio.
- Implementación basada en disco de una solución de protección de datos para varios sitios
Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea en dos sitios.

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

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

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



Esta solución de protección de datos proporciona las siguientes ventajas:

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

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

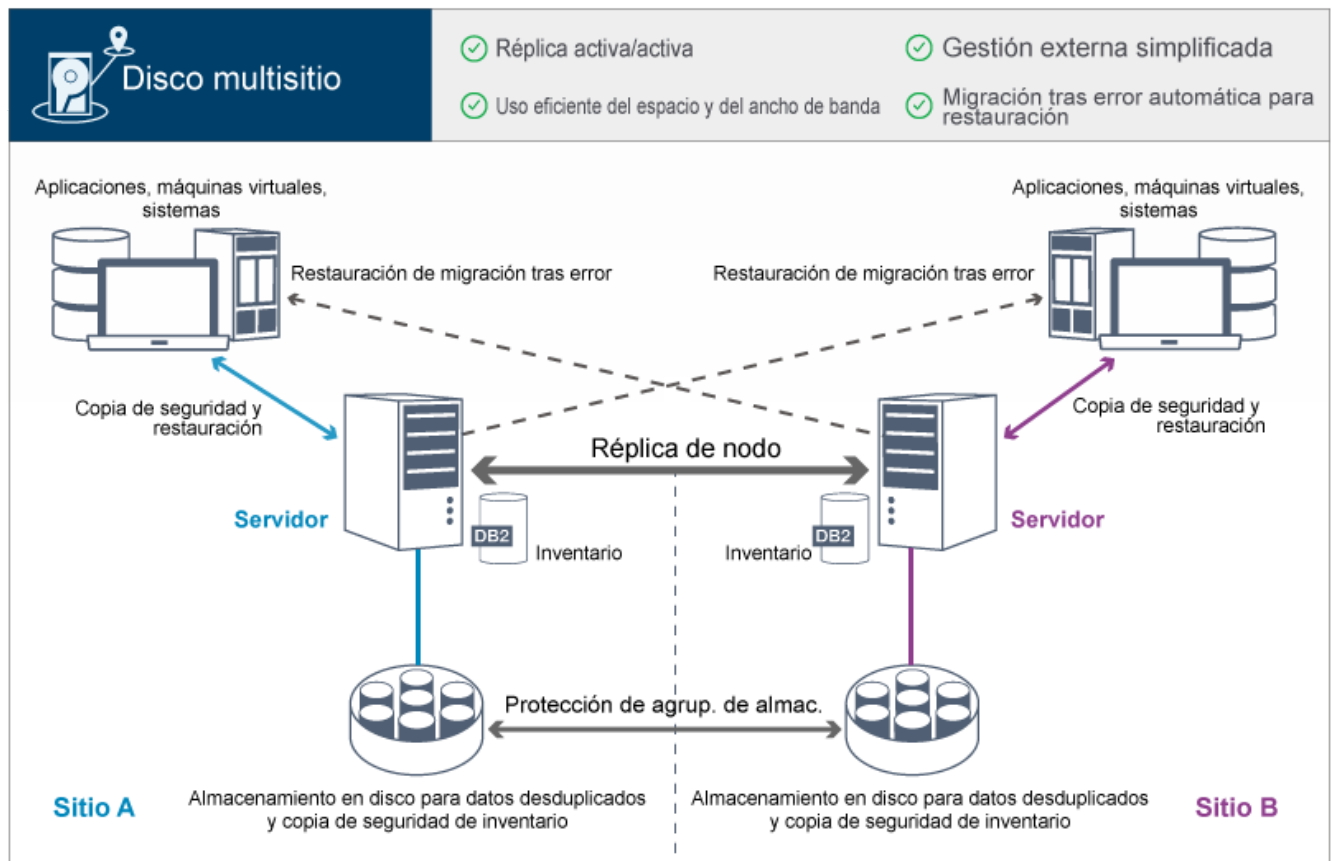
Referencia relacionada:

Comparación de soluciones de protección de datos

Hoja de ruta para implementar una solución de protección de datos

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

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



Esta solución de protección de datos proporciona las siguientes ventajas:

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

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

Referencia relacionada:

Comparación de soluciones de protección de datos
Hoja de ruta para implementar una solución de protección de datos

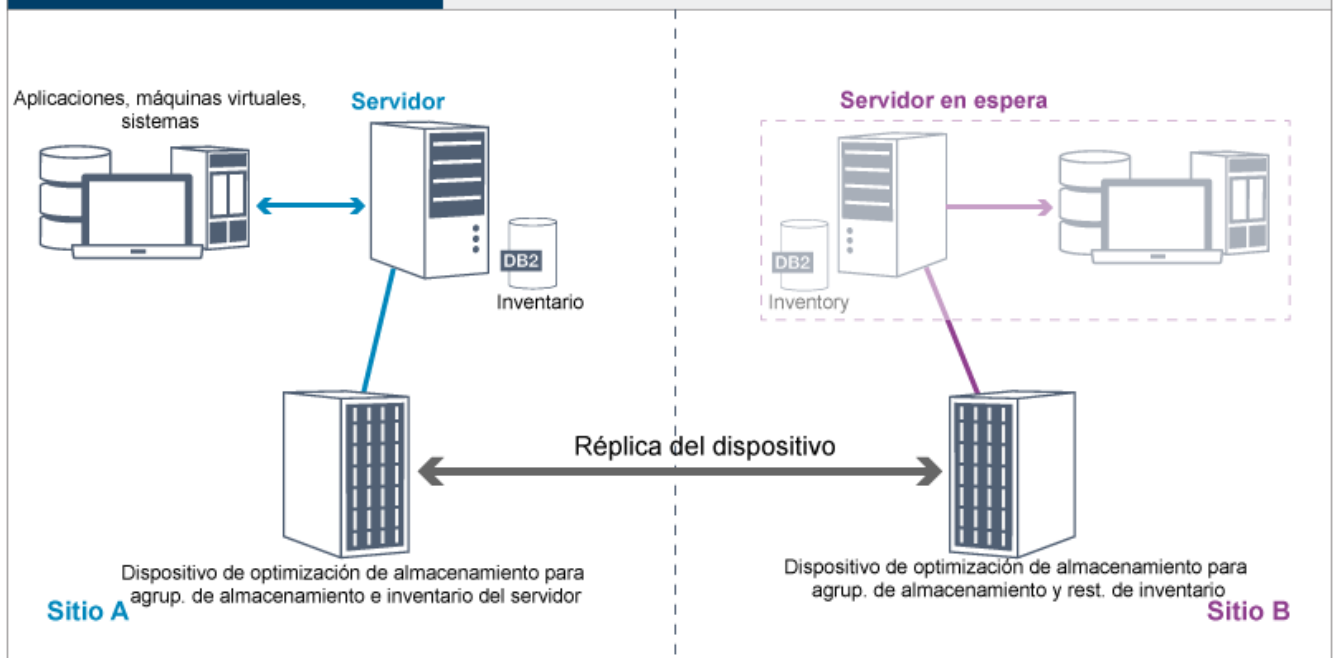
Implementación basada en dispositivo de una solución de protección de datos para varios sitios

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



Dispositivo multisitio

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



Esta solución de protección de datos proporciona las siguientes ventajas:

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

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

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

Referencia relacionada:

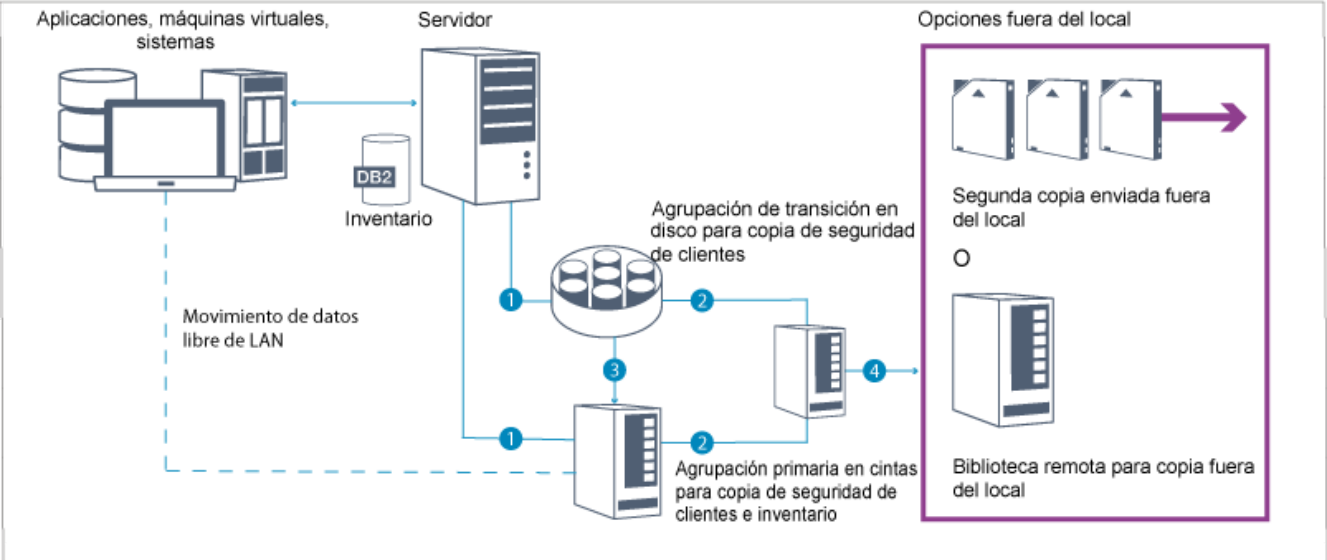
Comparación de soluciones de protección de datos
Hoja de ruta para implementar una solución de protección de datos

Implementación basada en cinta de una solución de protección de datos

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

Cinta

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



Esta solución de protección de datos proporciona las siguientes ventajas:

- Se optimiza el rendimiento para operaciones de copia de seguridad en redes de área de almacenamiento (SAN) de alta velocidad directamente a cinta para tipos de datos grandes y para retención de datos a largo plazo.
- Se optimiza el rendimiento para la disponibilidad de datos almacenando copias de datos en ubicaciones externas para la recuperación tras desastre. Si habilita la función de recuperación tras desastre y se produce un desastre, DRM le ayudará a agilizar el proceso de recuperación de sus servidores.
- La seguridad de los datos se ve optimizada al almacenar copias de los datos fuera del local en dispositivos de cinta que *no* están conectados a internet. Los ataques de ransomware se producen en las conexiones de internet; por lo tanto, el almacenamiento fuera del local puede ayudarle a protegerse ante dichos ataques.
- Se consigue una escalabilidad a bajo coste reduciendo la necesidad de hardware de disco adicional y disminuyendo los costes de energía.

Conceptos relacionados:

Seleccionar un controlador de dispositivo de cinta

Tareas relacionadas:

Creación de estrategias de copia de seguridad

Gestión del inventario de volúmenes

Referencia relacionada:





Comparación de soluciones de protección de datos

Instalación y configuración de controladores de dispositivos de cinta

Comparación de soluciones de protección de datos

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

	Disco de sitio único	Disco multisitio	Dispositivo multisitio	Cinta
Características destacadas				
Coste	\$	\$\$\$	\$\$\$\$	\$\$
Nivel de protección	Una copia de datos	Dos o más copias de datos	Dos o más copias de datos	Dos o más copias de datos

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

Acciones siguientes

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

Referencia relacionada:

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

Hoja de ruta para implementar una solución de protección de datos

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

Solución de disco de sitio único

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

Solución de disco multisitio

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

Solución de cinta

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

Solución de dispositivo multisitio

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

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

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

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

Referencia relacionada:

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

Solución de disco de sitio único

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

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

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

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

Opciones de implementación

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

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

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

Configure el servidor utilizando scripts automatizados

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

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

Hoja de vía de acceso de planificación

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



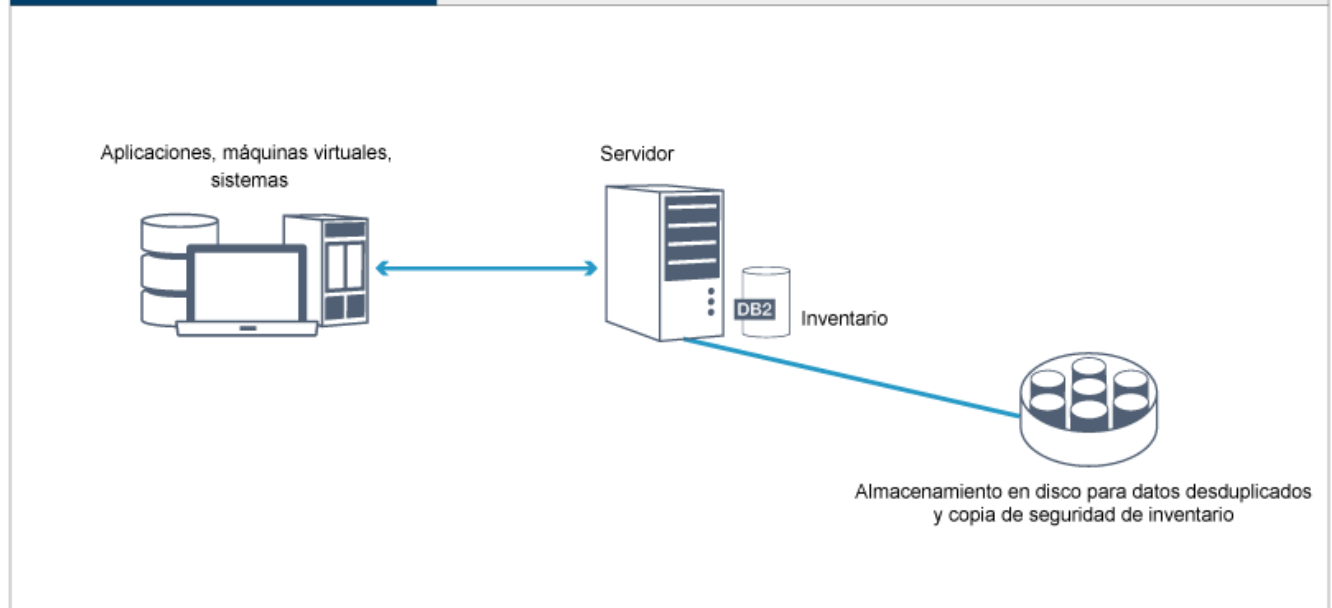
Disco de sitio único

✓ Arquitectura de un único sitio

✓ Precio ajustado

✓ Uso eficiente del espacio

✓ Implementación más sencilla



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

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

Selección de un tamaño del sistema

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

Acerca de esta tarea

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

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

Tabla 1. Determinación del tamaño del servidor

Total de datos gestionados	Cantidad diaria de datos nuevos de los que se debe hacer copia de seguridad	Tamaño de servidor necesario
60 TB - 240 TB	Hasta 10 TB al día	Pequeño
196 TB - 784 TB	10 - 20 TB al día	Mediano
1000 TB - 4000 TB	20 - 100 TB al día	Grande

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


Requisitos del sistema para una solución de disco de sitio único

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

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

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

Información relacionada:










 Sistemas operativos admitidos para IBM Spectrum Protect

Requisitos de hardware

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

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

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

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

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

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

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

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

Espacio de base de datos

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

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

Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 8 GB de espacio de registro de archivado cada 24 horas por cada 1000 clientes. En el ejemplo de 6500 clientes en el servidor concentrador y los servidores spoke, se utilizan 56 GB de espacio de registro de archivado a lo largo de un período de 24 horas para el servidor concentrador.

Para cada servidor de radio en el ejemplo, el espacio del registro de archivado que se utiliza a lo largo de 24 horas es aproximadamente 16 GB. Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en el requisito de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos:

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

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

Requisitos de software

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

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

Sistemas AIX

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

Sistemas Linux

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

Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS
Otro software	Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado. Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: <ul style="list-style-type: none">• Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada• Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador

Tareas relacionadas:

- ➔ Establecimiento de las opciones de red de AIX

Planificación de hojas de trabajo

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

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

Configuración previa de sistema servidor

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

Configuración del servidor

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

AIX

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

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
----------	----------------------	-------	-----------------------------	-------

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		50 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 2.
Directorio para la instalación del servidor	/		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/usr		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/var		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/tmp		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/opt		Espacio disponible que es necesario para el directorio: 10 GB	
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> • Pequeños y mediano: 140 GB • Grande: 300 GB 	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> • Pequeño: 1 TB • Medio: 2 TB • Grande: 4 TB 	

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

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

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

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

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

Linux

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

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

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

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

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

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

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

Windows

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

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

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

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

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

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

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

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

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

Planificación de almacenamiento

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

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

Base de datos y registro activo

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

Agrupación de almacenamiento

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

Referencia relacionada:

Planificación de la seguridad

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

Para obtener las directrices sobre la protección de entornos de almacenamiento ante ataques de ransomware y la recuperación de su entorno de almacenamiento en el caso de que se produzca un ataque, consulte Protección del entorno de almacenamiento ante ransomware.

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

Planificación de los roles de administración

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

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

Sistema

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

Política

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

Almacenamiento

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

Operador

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

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

Tabla 1. Escenarios para roles de administrador

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

Planificación para comunicaciones seguras

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

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

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

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

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

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

Tareas relacionadas:

[Protección de las comunicaciones](#)

Planificación de almacenamiento de datos cifrados

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

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

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

Información relacionada:

[Nota técnica 1963635](#)

Planificación del acceso de cortafuegos

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

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

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

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

Elemento	Valor predeterminado	Dirección	Descripción
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.
NDMP	No tiene valor predeterminado	Entrada/salida	<p>El servidor debe poder abrir una conexión de puerto de control NDMP de salida con el dispositivo NAS. El puerto de control de salida es la dirección de nivel inferior en la definición de transportador de datos para el dispositivo NAS.</p> <p>Durante una restauración NDMP de archivador a servidor, el servidor debe poder abrir una conexión de datos NDMP de salida con el dispositivo NAS. El puerto de conexión de datos que se utiliza durante una restauración puede configurarse en el dispositivo NAS.</p> <p>Durante las copias de seguridad NDMP de archivador a servidor, el dispositivo NAS debe poder abrir conexiones de datos de salida con el servidor y el servidor debe poder aceptar las conexiones de datos NDMP de entrada. Puede utilizar la opción de servidor NDMPORTRANGE para restringir el conjunto de puertos disponibles para su uso como conexiones de datos NDMP. Puede configurar un cortafuegos para conexiones a estos puertos.</p>
Réplica	No tiene valor predeterminado	Entrada/salida	<p>El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica.</p> <p>Los puertos de entrada para la réplica son los puertos TCP y SSL que el servidor de origen indique en el mandato DEFINE SERVER.</p>
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesión de ejecución larga	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente-servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	El puerto de servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

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

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

Hoja de ruta de la implementación

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

1. Configurar el sistema.
 - a. Configurar el hardware de almacenamiento y las matrices de almacenamiento para el tamaño del entorno.
 - b. Instalar el sistema operativo del servidor.
 - c. Configurar la E/S de multivía de acceso.

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

Configuración del sistema

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

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

Configuración del hardware de almacenamiento

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

Procedimiento

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

Instalación del sistema operativo del servidor

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

- Instalación en sistemas AIX
Complete los pasos siguientes para instalar AIX en el sistema servidor.
- Instalación en sistemas Linux
Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.
- Instalación en sistemas Windows
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

Instalación en sistemas AIX

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

Procedimiento

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

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

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

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

```
127.0.0.1 localhost
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<code>mode</code>	<code>8023ad</code>	
<code>auto_recovery</code>	<code>yes</code>	Habilitar la recuperación automática tras la migración tras error.
<code>backup_adapter</code>	<code>NONE</code>	Adaptador utilizado cuando falla todo el canal.

hash_mode	src_dst_port	Determina cómo se elige el adaptador saliente.
interval	long	Determina el valor de intervalo para IEEE.
mode	8023ad	Modalidad de 802.3ad Modalidad de funcionamiento de EtherChannel
netaddr	0	Dirección para el ping
noloss_failover	yes	Habilitar migración tras error sin pérdidas tras anomalía del ping
num_retries	3	Veces que reintentar el ping antes de considerarlo un error
retry_time	1	Tiempo de espera (en segundos) entre pings
use_alt_addr	no	Habilitar dirección EtherChannel alternativa
use_jumbo_frame	no	Habilitar tramas de gran tamaño de Gigabit Ethernet

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

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

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

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

Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.

Antes de empezar

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

Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
 - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
 - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
 - c. Seleccione las preferencias de idioma y teclado.
 - d. Seleccione la ubicación para establecer el huso horario correcto.
 - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
 - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:

- El disco local de 300 GB se ha seleccionado como destino de instalación.
- En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.

Pulse Terminado.

g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root. Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato df para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

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

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

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

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

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

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

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

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

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

```
127.0.0.1 localhost
```

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

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

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

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

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

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

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

Si el directorio repos.d no existe, créelo.

- Liste el contenido de directorio:

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

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

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

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

```
vi rhel71_dvd.repo
```

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

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

h. Instale el paquete de requisito previo ksh.x86_64, emitiendo el mandato yum. Por ejemplo:

```
yum install ksh.x86_64
```

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

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

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

```
umount /mnt
```

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

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

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

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

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

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

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

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

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

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

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

Tabla 1. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción
kernel.shmmni	El número máximo de segmentos.
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes). Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas).
kernel.sem	(SEMMSL)
Hay cuatro valores para el parámetro kernel.sem.	El número máximo de semáforos por matriz.
	(SEMMNS)
	El número máximo de semáforos por sistema.
	(SEMOPM)
	El número máximo de operaciones por llamada a semáforo.
	(SEMMNI)
	El número máximo de matrices.
kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema.
kernel.msgmax	Tamaño máximo de los mensajes (bytes).
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes).

Parámetro	Descripción
kernel.randomize_va_space	El parámetro kernel.randomize_va_space configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.
vm.swappiness	El parámetro vm.swappiness define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.
vm.overcommit_memory	El parámetro vm.overcommit_memory influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.

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

- a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.
Emita el mandato siguiente:

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

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

Emita el mandato siguiente:

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

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

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

Emita el mandato siguiente:

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

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

Emita el mandato siguiente:

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

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

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

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

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

Instalación en sistemas Windows

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

Procedimiento

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

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

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

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

Configuración de E/S de la multivía de acceso

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

- Sistemas AIX
- Sistemas Linux
- Sistemas Windows

Sistemas AIX

Procedimiento

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

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

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

- En sistemas grandes, emita los siguientes mandatos:

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

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

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

- o devices.fcp.disk.rte
3. Emita el mandato `cfgmgr` para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

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

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

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

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

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

```
lspv -u
```

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

```
hdisk4 00f8cf083fd97327 None active
3321360050763008101057800000000000003004214503IBMfcp
```

En el ejemplo, `6005076300810105780000000000030` es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

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

```
bootinfo -s hdisk4
```

Sistemas Linux

Procedimiento

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

```
mpathconf --enable
```

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

```
defaults {
    user_friendly_names no
}

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

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

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

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

```
multipath -l
```

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

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
  size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
|  `-- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
   |- 1:0:1:18 sdat 66:208   active undef running
   `-- 3:0:0:18 sddy 128:0   active undef running
```

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

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

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

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

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

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 36005076802810c509800000000000012.

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

Sistemas Windows

Procedimiento

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.

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

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

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

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

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

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

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

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

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

Creación del ID de usuario para el servidor

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



Acerca de esta tarea

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


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

Procedimiento

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

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

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


 **Sistemas operativos AIX**

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

 **Sistemas operativos Linux**

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

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

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

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

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

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

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

Preparación de sistemas de archivos para el servidor

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

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

Preparación de sistemas de archivos en sistemas AIX

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

Procedimiento

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

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

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

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

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

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

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

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

Por ejemplo:

```
lsvg -p tsmdb
```

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

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

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

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

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

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

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

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

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

```
mount -a
```

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

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

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

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

Preparación de sistemas de archivos en sistemas Linux

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

Procedimiento

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

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

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

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

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

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

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

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

```
mkdir /tsminst1
```

Repita el mandato mkdir para cada sistema de archivos.

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

Por ejemplo:

```
/dev/mapper/36005076802810c50980000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

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

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G   1%  /tsminst1/TSMalog
```

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

Preparación de sistemas de archivos en sistemas Windows

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

Procedimiento

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

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

```
md c:\tsminst1
```

Repita el mandato md para cada sistema de archivos.

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

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

- a. Ponga el disco en línea.
- b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
- c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como TSMfile00. No asigne el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como C:\tsminst1\TSMfile00.
Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.

3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato mountvol y, a continuación, revise la salida. Por ejemplo:

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

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

Qué hacer a continuación

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

Instalación del servidor y Centro de operaciones

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

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

Instalación en sistemas AIX y Linux

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

Antes de empezar

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

Procedimiento

1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.

Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.


2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

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

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package_name* es el nombre del archivo descargado.

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

```
lsuser
```

De manera predeterminada, el mandato está habilitado.

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

```
./install.sh
```

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



Qué hacer a continuación

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

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

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

Tareas relacionadas:

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

Instalación en sistemas Windows

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

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos previos:

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

Procedimiento

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.

5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.


Qué hacer a continuación

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

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

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

Tareas relacionadas:

 Otros métodos para instalar componentes de IBM Spectrum Protect

Configuración del servidor y el Centro de operaciones

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

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

Configuración de la instancia de servidor

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

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.

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




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



1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
 - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
 - b. Seleccione Configuración avanzada.
 - c. Seleccione Reglas de entrada.
 - d. Seleccione Nueva regla.
 - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
 - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
 - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
 - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
 - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada > Inhabilitar > Aceptar.
4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.


Acerca de esta tarea

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

Procedimiento

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

 Sistemas operativos AIX  Sistemas operativos Linux En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.

 Sistemas operativos Windows Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

Instalación del cliente de archivado y copia de seguridad

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

Procedimiento

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

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

Configuración de opciones para el servidor

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

Procedimiento

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

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Sí	No	No
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

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

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

```
setopt idletimeout 60
```

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

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

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

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

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

Referencia relacionada:

- Referencia de opciones de servidor
- SETOPT (Establecer una opción de servidor para actualización dinámica)

Configuración de comunicaciones seguras con Seguridad de la capa de transporte

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

Acerca de esta tarea

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



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

Configuración de Centro de operaciones

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

Antes de empezar

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

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

Procedimiento

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

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

donde:

- nombre_host representa el nombre del sistema donde está instalado Centro de operaciones
- puerto_seguro representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

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

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

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

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

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

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

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

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

Registro de la licencia de producto


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

Acerca de esta tarea

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

Procedimiento


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

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

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

Qué hacer a continuación

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

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

Referencia relacionada:

 REGISTER LICENSE (Registrar una nueva licencia)

Configuración de la optimización de almacenamiento de datos

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

Antes de empezar

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

Procedimiento

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el cursor por encima de Almacenamiento.
3. En la lista que se visualiza, pulse Agrupaciones de almacenamiento.
4. Pulse el botón +Agrupación de almacenamiento.

5. Complete los pasos del asistente Añadir agrupación de almacenamiento:
 - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
 - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
6. Tras configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.

Definición de las reglas de retención de datos para su empresa

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

Procedimiento

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

Tareas relacionadas:

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

Definición de planificaciones para actividades de mantenimiento del servidor

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

Acerca de esta tarea

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

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

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



Procedimiento

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


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

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

donde *directorios_copia_seguridad_bd* es una lista de los directorios que ha creado para la copia de seguridad de base de datos.

 Sistemas operativos AIX  Sistemas operativos Linux Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando por el mandato /tsminst1/TSMbkup00, emita el mandato siguiente:

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

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

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

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

```
set dbrecovery dbback_filedev
```

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

Operación	Mandato de ejemplo
Realizar una copia de seguridad de la base de datos.	<p>Cree una planificación para ejecutar el mandato BACKUP DB. Si está configurando un sistema pequeño, establezca el parámetro COMPRESS en YES.</p> <p>Por ejemplo, en un sistema pequeño, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes</pre>
Realice una copia de seguridad de la información de configuración del dispositivo.	<p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
Haga una copia de seguridad del historial de volumen.	<p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>

Operación	Mandato de ejemplo
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	<p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>
Elimine objetos que exceden su retención permitida.	<p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY. Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar:</p> <ul style="list-style-type: none"> o Sistemas pequeños: 10 o Sistemas medianos: 30 o Sistemas grandes: 40 <p>Por ejemplo, en un sistema de tamaño mediano, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes</pre>

Qué hacer a continuación

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

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

Referencia relacionada:

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

Definición de planificaciones de cliente

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

Procedimiento

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

Instalación y configuración de clientes de archivado y copia de seguridad

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

Procedimiento

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

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

Qué hacer a continuación

Registrar y asignar los clientes a planificaciones.

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

Registro y asignación de clientes a planificaciones

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

Antes de empezar

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

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

Procedimiento

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

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

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

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

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

Instalación del servicio de gestión de cliente

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

Procedimiento

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

1. Descargue el paquete de instalación para el servicio de gestión de cliente desde un sitio de descarga de IBM® como por ejemplo IBM Passport Advantage® o IBM Fix Central. Busque un nombre de archivo que sea similar a *<versión>-IBM_Spectrum_Protect-CMS-sistema_operativo.bin*.
2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
3. Extraiga el contenido del archivo del paquete de instalación.

4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
5. Para instalar el servicio de gestión de cliente, siga las instrucciones del asistente del Gestor de instalación de IBM. Si el Gestor de instalación de IBM no está instalado en el sistema cliente, debe seleccionar el Gestor de instalación de IBM y los Servicios de gestión de cliente de IBM Spectrum Protect.
 - Verificación de que el servicio de gestión de clientes está instalado correctamente
Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.
 - Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente
Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

Tareas relacionadas:

 Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas

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

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

Procedimiento

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

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

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

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

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

La salida es similar al texto siguiente:

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

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

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

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

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

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

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

```
C:\Program Files\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

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

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
             en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo client-configuration.xml. Para obtener instrucciones para configurar este archivo, consulte Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato CmsConfig verify para comprobar que una definición de nodo se ha creado correctamente en el archivo client-configuration.xml.

Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente

Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

Antes de empezar

Asegúrese de que el servicio de gestión de cliente está instalado y se ha iniciado en el sistema cliente. Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de cliente no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
 - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse por una red, mientras que el servicio de gestión de cliente se comunica por la otra red.
 - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, se le asigna dinámicamente al sistema cliente una dirección IP, que se guarda en el servidor durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

Procedimiento

Para configurar Centro de operaciones para utilizar el servicio de gestión de cliente, complete los pasos siguientes:

1. En la página Clientes de Centro de operaciones, seleccione el cliente.
2. Pulse Detalles > Propiedades.
3. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de cliente en el sistema cliente. La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	https://server.example.com
Con el nombre de host de DNS y puerto no predeterminado	https://server.example.com:1599
Con la dirección IP y puerto no predeterminado	https://192.0.2.0:1599

4. Pulse Guardar.

Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

Procedimiento

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
 - a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
 - b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
 - c. Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.
Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.
2. Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de disco de sitio único.

Supervisión de una solución de disco de sitio único

Después de implementar una solución de disco en un único sitio con IBM Spectrum Protect, supervise la solución para su funcionamiento correcto. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

Acerca de esta tarea

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar un informe de correo electrónico diario que resume el estado del sistema.

En algunos casos, es posible que desee utilizar herramientas de supervisión avanzadas para completar tareas de supervisión o resolución de problemas específicas.

Consejo: Si piensa diagnosticar problemas con clientes de archivado y copia de seguridad en sistemas operativos Linux o Windows, instale los servicios de gestión de cliente de IBM Spectrum Protect en cada sistema donde esté instalado un cliente de archivado y copia de seguridad. De esta forma, puede garantizar que el botón Diagnosticar está disponible en Centro de operaciones para diagnosticar problemas con los clientes de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.

Procedimiento

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación diaria.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación de supervisión periódica.
3. Para verificar que la solución de IBM Spectrum Protect cumple con los requisitos de licencia, siga las instrucciones que encontrará en Verificación de la conformidad de licencia.
4. Si desea configurar el Centro de operaciones para generar informes de estado de correo electrónico, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

Qué hacer a continuación

Resuelva cualquier problema que encuentre. Para resolver un problema cambiando la configuración de la solución, siga las instrucciones que encontrará en Gestión de operaciones para una solución de disco de sitio único. Los siguientes recursos están también disponibles:

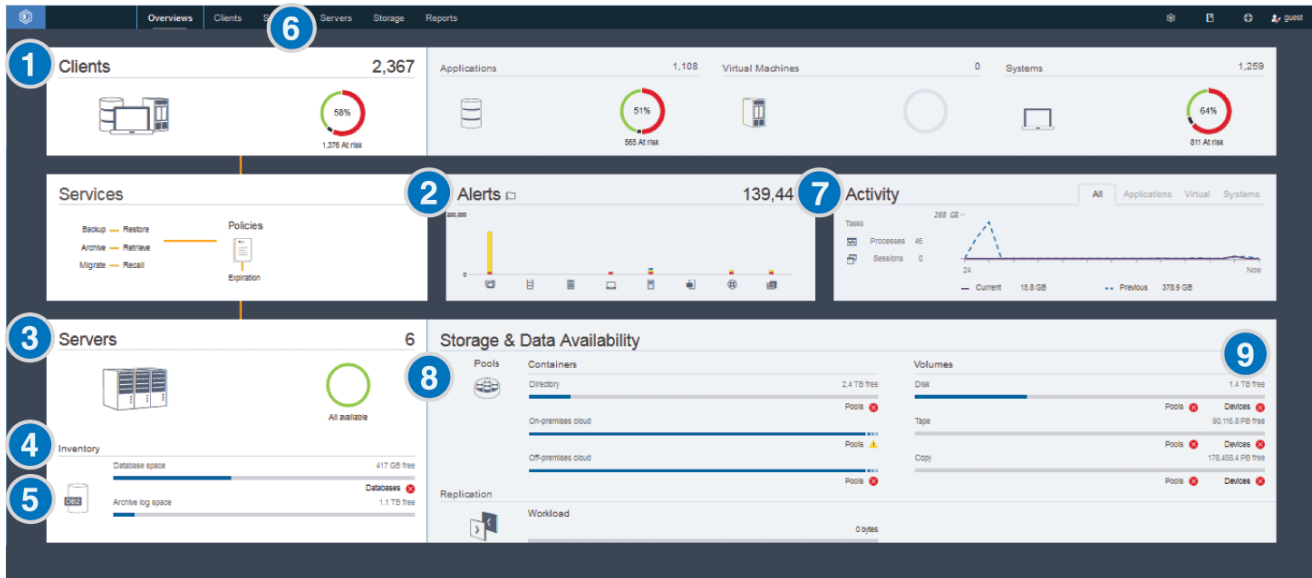
- Para resolver problemas de rendimiento, consulte Rendimiento.
- Para resolver otros tipos de problemas, consulte Resolución de problemas.


Lista de comprobación de supervisión diaria

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.








Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.


La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.

Tabla 1. Tareas de supervisión diarias



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>1 Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Atención: Si el porcentaje En riesgo es superior al habitual, es posible que indique que se ha producido un ataque de ransomware. Un ataque de ransomware puede hacer que las operaciones de copia de seguridad fallen, poniendo a los clientes en una situación de riesgo. Por ejemplo, si el porcentaje de clientes en riesgo se encuentra habitualmente entre un 5% y un 10%, pero el porcentaje se incrementa a un 40% o 50%, investigue la causa. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Clientes, seleccione el cliente y pulse Detalles. 2. Para diagnosticar un problema, pulse Diagnóstico. 	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>2 Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Alertas. 2. En la tabla Alertas, seleccione una alerta. 3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.
<p>3 Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> 1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible. 2. Para ver información adicional, pulse el área Servidores. 3. Seleccione un servidor en la tabla Servidores y pulse Detalles. 	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione un servidor y pulse Detalles. 2. Para actualizar las propiedades de servidor, pulse Propiedades.

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado. o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor. o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio. o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC. o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio. 	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>5 Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos. 	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione una fila y pulse Detalles. 2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad. <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Servidores. 2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad. <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Emita el mandato QUERY DB: <pre>query db f=d</pre> 3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.
<p>6 Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse Servidores > Mantenimiento. 2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial. 3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso. 	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>7 Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> • Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad. • Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores. 	<ul style="list-style-type: none"> • Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente. Atención: Si la cantidad de datos de copia de seguridad es significativamente superior a lo habitual, puede que indique un ataque de ransomware. Cuando un ransomware cifra datos, el sistema percibe que se están cambiando los datos, y realiza una copia de seguridad de los datos cambiados. Así, los volúmenes de copia de seguridad se vuelven más grandes. Para determinar qué clientes están afectados, pulse los separadores Aplicaciones, Virtual o Sistemas. • Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>8 Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<p>1. Si se indican problemas en el área Almacenamiento & Disponibilidad de datos, pulse Agrupaciones para ver los detalles:</p> <ul style="list-style-type: none"> ○ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible. Atención: Si el estado es crítico, investigue la causa: <ul style="list-style-type: none"> ■ Si el índice de deduplicación de datos para una agrupación de almacenamiento cae significativamente, puede indicar un ataque de ransomware. Durante un ataque de ransomware, se cifran los datos y estos no podrán ser deduplicados. Para verificar el índice de deduplicación de datos, en la tabla Agrupaciones de almacenamiento, revise el valor de la columna % de ahorro. ■ Si la agrupación de almacenamiento muestra inesperadamente un uso del 100%, esto puede indicar un ataque de ransomware. Para verificar la utilización, revise el valor de la columna Capacidad utilizada. Pase el cursor por encima de los valores para ver los porcentajes de espacio utilizado y libre. ○ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura. <p>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</p>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento & Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> • En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes. • En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios. • Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.

Lista de comprobación de supervisión periódica

Para asegurarse de que la solución IBM Spectrum Protect opera correctamente, complete las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.










Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>. Busque el servidor asociado al cliente. 2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>. 3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>. 4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones que encontrará en QUERY ACTLOG (Consultar las anotaciones de actividades). 5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa. <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>. 2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>. 3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>. 	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento comunes del cliente</i>.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> 1. En la página <i>Centro de operaciones Descripción general</i>, pulse <i>Agrupaciones</i>. 2. Seleccione una agrupación y pulse <i>Vista rápida</i>. 3. En el área <i>Optimización de almacenamiento de datos</i>, vea la fila <i>Espacio guardado</i>. 	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores de nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la página <i>Descripción general de Centro de operaciones</i>, pase el ratón sobre el icono de configuración  y pulse <i>Creador de mandatos</i>. 2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones que encontrará en GENERATE DEDUPSTATS (Generar estadísticas de deduplicación de datos respecto a una agrupación de almacenamiento de contenedores de directorio). 3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones que encontrará en QUERY DEDUPSTATS (Consultar las estadísticas de deduplicación de datos).

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory query option devconfig</pre> 3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo. <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	




Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine si está disponible espacio suficiente para el sistema de archivos del directorio de la instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad. <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX •  Sistemas operativos Linux /home/tsminst1/tsminst1 •  Sistemas operativos Windows C:\tsminst1 <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Clientes. 2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente. 3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades. 4. En el área Última sesión, visualice la fila Enviado a cliente. 	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p> <p>Revise de forma periódica la tabla de resumen de actividad SQL, que contiene estadísticas sobre las sesiones de cliente. Para comparar la actividad actual con la actividad previa, utilice una sentencia SQL SELECT. Si el nivel de actividad es significativamente diferente de la actividad anterior, puede que indique un ataque de ransomware.</p> <p>Revise de forma periódica el registro de actividad. Busque los mensajes de ANE que indican a cuántos archivos se les realizó copia de seguridad y fueron inspeccionados. Compare los índices de deduplicación de los datos actuales con los índices anteriores. Si se realizó una copia de seguridad a un número de archivos más alto de lo habitual, o el índice de deduplicación cae de forma inesperada a 0, puede indicar un ataque de ransomware.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones. 2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles. 	<p>Sugerencias:</p> <ul style="list-style-type: none"> • Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. 3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>. • Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>. • Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> • Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes > Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones. 2. Seleccione una planificación y pulse Detalles. 3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila. 4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado. 5. Pulse Guardar.
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores > Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).

Referencia relacionada:

-  [QUERY ACTLOG](#) (Consultar las anotaciones de actividades)
-  [UPDATE STGPOOL](#) (Actualizar una agrupación de almacenamiento)
-  [QUERY EXTENTUPDATES](#) (Consultar extensiones de datos actualizadas)

Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

Licencia de PVU



El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.

Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia. Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
Modelo frontal	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
Modelo suplementario	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
Modelo de PVU	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.</p>

Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.

- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

Procedimiento


Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

Resultados

Los informes habilitados se envían según los valores especificados.

Referencia relacionada:

 [UPDATE ADMIN \(Actualizar un administrador\)](#)

Gestión de operaciones para una solución de disco de sitio único

Utilice esta información para gestionar operaciones para una solución de disco de sitio único con IBM Spectrum Protect que incluya un servidor y utilice la eliminación de datos duplicados para una única ubicación.

- **Gestión del Centro de operaciones**
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.
- **Protección de aplicaciones, máquinas virtuales y sistemas**
El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.
- **Gestión del almacenamiento de datos**
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Protección del servidor IBM Spectrum Protect**
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Implementación de un plan de recuperación tras desastre**
Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.
- **Recuperación de paradas del sistema**
Para soluciones de disco de sitio único de IBM Spectrum Protect, puede recuperar el inventario localmente únicamente y restaurar la base de datos para proteger los datos.

Gestión del Centro de operaciones

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Reinicio del asistente de configuración inicial
Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.
- Cambio del servidor concentrador
Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.
- Restauración de la configuración a un estado de preconfiguración
Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Adición y eliminación de servidores spoke

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

Acerca de esta tarea

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke
Puede eliminar un servidor spoke del Centro de operaciones.

Adición de un servidor de radio

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

Antes de empezar

Las comunicaciones entre el servidor spoke y el servidor concentrador deben asegurarse utilizando el protocolo de Seguridad de la capa de transporte (TLS). Para asegurar las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

Procedimiento

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
 - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
 - Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.

Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente a 14 días, si configura el servidor como un servidor de radio.

Eliminación de un servidor spoke

Puede eliminar un servidor spoke del Centro de operaciones.

Acerca de esta tarea

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

Procedimiento

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre_grupo* representa el nombre del grupo supervisado y *nombre_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```

Consejo: Si se suprime una definición de servidor inmediatamente después de que se haya eliminado del grupo supervisado, la información de estado del servidor puede permanecer en el Centro de operaciones indefinidamente.


Para evitar este problema, espere a que pase el intervalo de recopilación de estados antes de suprimir la definición de servidor. El intervalo de recopilación de estados se muestra en la página Valores del Centro de operaciones.

Inicio y detención del servidor web

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.

Procedimiento

1. Detener el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation_dir/ui/Utils*, donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:


```
./stopserver.sh
```

-  Sistemas operativos Linux Emita el mandato siguiente:


```
service opscenter.rc stop
```

-  Sistemas operativos Windows En la ventana Servicios, detenga el servicio de IBM Spectrum Protect Operations Center.

2. Inicie el servidor web.

-  Sistemas operativos AIX Desde el directorio `/installation_dir/ui/utls`, donde `installation_dir` representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

```
./startserver.sh
```

-  Sistemas operativos Linux Emita los mandatos siguientes:

Inicie el servidor:


```
service opscenter.rc start
```

Reinicie el servidor:

```
service opscenter.rc restart
```

Determine si el servidor se está ejecutando:

```
service opscenter.rc status
```

-  Sistemas operativos Windows En la ventana Servicios, inicie el servicio IBM Spectrum Protect Operations Center.

Reinicio del asistente de configuración inicial

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

Antes de empezar

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:







- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.

Acerca de esta tarea

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

Procedimiento

1. Detenga el servidor web de Centro de operaciones.
 2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde `installation_dir` representa el directorio en el que está instalado Centro de operaciones:
 -  Sistemas operativos AIX  Sistemas operativos Linux `dir_instalación/ui/Liberty/usr/servers/guiServer`
 -  Sistemas operativos Windows `dir_instalación\ui\Liberty\usr\servers\guiServer`
- Por ejemplo:
-  Sistemas operativos AIX  Sistemas operativos Linux `opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer`
 -  Sistemas operativos Windows `c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer`
3. En el directorio `guiServer`, elimine el archivo `serverConnection.properties`.
 4. Inicie el servidor web Centro de operaciones.
 5. Abra el Centro de operaciones.
 6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
 7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

Cambio del servidor concentrador

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

Procedimiento

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

Tareas relacionadas:

Reinicio del asistente de configuración inicial

Restauración de la configuración a un estado de preconfiguración

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Procedimiento

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
 - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
 - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restaure los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.

Tareas relacionadas:

Reinicio del asistente de configuración inicial

Inicio y detención del servidor web

Protección de aplicaciones, máquinas virtuales y sistemas

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Gestión de operaciones de cliente
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.
- Gestión de actualizaciones del cliente
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- Poner fuera de servicio un nodo cliente
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- Desactivación de datos para liberar espacio de almacenamiento
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Adición de clientes

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

Acerca de esta tarea

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones que encontrará en Selección del software de cliente y planificación de la instalación.
2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones que encontrará en Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones que encontrará en Instalación y configuración de clientes.

Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

Acerca de esta tarea

La práctica preferida es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente para poder configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración en la documentación de producto para asegurarse de que se puede producir las operaciones planificadas.

Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de archivado y copia de seguridad realiza la copia de seguridad y el archivado de archivos y directorios de los servidores de archivos y las estaciones de trabajo en el almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none">• Requisitos del cliente de archivado y copia de seguridad• Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux• Instalación del cliente de archivado y copia de seguridad de Windows

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM software de base de datos DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se han completado sin concluir servidores IBM Domino.	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se han completado sin concluir servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de DB2 en el servidor IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de Informix en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection for SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales almacenadas en un servidor centralizado, crear políticas de copia de seguridad y restaurar máquinas virtuales o archivos individuales.</p> <p>De forma alternativa, utilice el cliente de archivado y copia de seguridad para hacer la copia de seguridad y restauración de una máquina virtual de VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> • Instalación de Data Protection for Microsoft Hyper-V • Instalación y actualización de Data Protection for VMware • Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

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

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

Acerca de esta tarea

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el periodo de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro de cliente, se asigna un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activas* activo.

Cuando un cliente realiza la copia de seguridad o el archivado de un archivo, el archivo se vincula a una clase de gestión del conjunto de políticas activas activo del dominio de políticas. Una *clase de gestión* es el conjunto de claves de reglas para gestionar los datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo local editable del sistema cliente y en un conjunto de opciones de cliente en el servidor. Las opciones del conjunto de opciones de cliente en el servidor pueden alterar temporalmente las opciones del archivo de opciones del cliente local o añadirse a dichas opciones.

Procedimiento

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

Visualización de políticas

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

Procedimiento

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
 - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
Consejo: Para ayudar a garantizar que pueda recuperar los datos después de un ataque de ransomware, aplique las siguientes directrices:
 - Asegúrese de que el valor de la columna de copias de seguridad tiene un valor mínimo de 2. El valor preferido es 3, 4 o más.

- Asegúrese de que el valor en la columna Mantener copias de seguridad extra tiene un valor mínimo de 14 días. El valor preferido es 30 o más días.
 - Asegúrese de que el valor de la columna Mantener archivados tiene un valor mínimo de 30 días.
- Si el software de IBM Spectrum Protect for Space Management está instalado en el cliente, asegúrese de que se ha realizado una copia de seguridad de los datos antes de realizar la migración. En el mandato DEFINE MGMTCLASS o UPDATE MGMTCLASS, especifique MIGREQUIRESBKUP=YES. A continuación, siga las directrices de la sugerencia.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
 - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
 - c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

Edición de políticas

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
Añadir una clase de gestión	<ol style="list-style-type: none"> a. En la tabla Conjuntos de políticas, pulse +Clase de gestión. b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión. c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada. d. Pulse Añadir.
Suprimir una clase de gestión	<p>En la columna Clase de gestión, pulse -.</p> <p>Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.</p>

Opción	Descripción
Establecer una clase de gestión como clase de gestión predeterminada	En la columna Predeterminada para la clase de gestión, pulse el botón de selección. Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.
Modificar una clase de gestión	Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.

6. Pulse Guardar.

Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.

7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas.

Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:

- Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
- Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.
- Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


Procedimiento

- Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menús Centro de operaciones. Pulse Planificaciones.
- Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
Modificar una planificación	<ol style="list-style-type: none"> En la vista Planificaciones, seleccione la planificación y pulse Detalles. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas. Modifique los valores de la planificación y pulse Guardar.
Crear una planificación	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
 - a. En la página Visión general del Centro de operaciones, pase el ratón por encima del icono de configuración  y pulse Creador de mandatos.
 - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

Tareas relacionadas:

-  Ajuste de la planificación para las operaciones diarias

Registro de clientes

Registrar un cliente para garantizar que el cliente pueda conectarse con el servidor y el servidor pueda proteger los datos de cliente.

Antes de empezar

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

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

Procedimiento

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





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

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

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

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

Referencia relacionada:

-  Opción Tcpserveraddress
-  Opción Tcppport
-  Opción Nodename
-  Opción Deduplication

Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:

- o Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"> ■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux ■ Instalación del cliente de archivado y copia de seguridad de Windows <p>Consejo: También puede actualizar los clientes existentes utilizando el Centro de operaciones. Para obtener instrucciones, consulte Planificación de actualizaciones del cliente.</p>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> ■ Instalación de Data Protection for Oracle ■ Instalación de Data Protection for SQL Server en Windows Server Core
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> ■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) ■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) ■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> ■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux ■ Instalación y actualización de IBM Spectrum Protect Snapshot for VMware ■ Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- o Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> ■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux ■ Instalación del cliente de archivado y copia de seguridad de Windows
Si planea crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo de cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> ■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSEVERADDRESS, TCPPOINT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (Registro de clientes).
 - o Para los clientes que están instalados en un sistema operativo AIX, Linux o Mac OS X, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
 - o Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt.

De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de clientes en el cliente. Siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones que encontrará en Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones que encontrará en Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:

- a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
 - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

Qué hacer a continuación

Si necesita cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones que encontrará en Modificación del ámbito de una copia de seguridad de cliente.

Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

Acerca de esta tarea

El método preferido es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Utilizando el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que las operaciones planificadas se pueden producir.

Si la empresa utiliza una herramienta de planificación de terceros como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Normalmente, las herramientas de planificación de terceros inician los programas cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

Procedimiento

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones para el sistema operativo que está instalado en el nodo cliente.

AIX y Oracle Solaris

- a. Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Pulse la pestaña Cliente web.
- c. En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- d. Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo dsm.sys, establezca la opción passwordaccess en generate.
- e. Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- f. Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- g. Para permitir que el aceptador de cliente se inicie automáticamente después del reinicio de un sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, /etc/inittab):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```


Linux

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo dsm.sys, establezca la opción passwordaccess en generate.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente iniciando sesión con el ID de usuario root y emitiendo el mandato siguiente:

```
service dsmcad start
```

- Para permitir que el aceptador de cliente pueda iniciarse automáticamente después del reinicio de un sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

MAC OS X

- En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

Windows

- En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- Consulte la información en la página Asistente del planificador y pulse Siguiente.
- En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- Complete la configuración paso a paso a través del asistente.
- Actualice el archivo de opciones de cliente, dsm.opt, y configure la opción passwordaccess como generate.
- Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El servicio de planificador se ha iniciado y detenido automáticamente mediante el servicio aceptador de cliente, según sea necesario.

Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

Antes de empezar

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores de opción en el archivo de opciones de cliente que ha obtenido durante ese proceso. Puede utilizar los valores para especificar puertos.

Acerca de esta tarea

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

Procedimiento

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción `tcpport` en el archivo de opciones de cliente. La opción `tcpport` del archivo de opciones de cliente debe coincidir con la opción `TCPPORT` en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción `httpport` en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción `webports` en el archivo de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción `tcpadminport` de cliente debe coincidir con el valor de la opción de servidor `TCPADMINPORT`. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.

Gestión de operaciones de cliente

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

Acerca de esta tarea

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- Evaluación de errores en registros de errores de cliente
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- Detención y reinicio del aceptador de cliente
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- Restablecimiento de contraseñas
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- Modificación del ámbito de una copia de seguridad de cliente
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Evaluación de errores en registros de errores de cliente

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

Antes de empezar

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que el servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación [Instalación del servicio de gestión de cliente](#). Para obtener instrucciones sobre cómo verificar la instalación, consulte [Verificación de que el servicio de gestión de clientes está instalado correctamente](#).

Procedimiento

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si el servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
 1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
 2. Pulse Detalles.
 3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
 4. Revise los mensajes de registro recuperados.

Sugerencias:

 - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
 - Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

 5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si el servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

Detención y reinicio del aceptador de cliente

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

Acerca de esta tarea

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

Procedimiento

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
 - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmscad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmscad
```


- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmscad
```

Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Iniciar y Aceptar.

Referencia relacionada:

 Resolución de problemas de planificación del cliente

Restablecimiento de contraseñas

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

Procedimiento

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:
 1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:


```
update node nombre_nodo nueva_contraseña forcepwreset=yes
```

donde *nombre_nodo* especifica el nodo cliente y *nueva_contraseña* especifica la contraseña que asigne.
 2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como generar en el archivo de opciones del cliente.
- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:
 1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
 2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:


```
update admin nombre_admin nueva_contraseña forcepwreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva_contraseña* especifica la contraseña que asigne.
- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:
 1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
 2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
 3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwreset=yes
```

donde *nombre_nodo* especifica el nombre del nodo y *nueva_contraseña* especifica la contraseña que asigne.

- Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

Modificación del ámbito de una copia de seguridad de cliente

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Acerca de esta tarea

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones que encontrará en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Para obtener información detallada al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción `dominio`. Siga las instrucciones que encontrará en Opción de cliente `Domain`.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

Antes de empezar

- Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
- Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
- Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none">Planificación de actualizaciones del cliente

Software	Enlace a instrucciones
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> • Actualización de Data Protection for SQL Server • Instalación de Data Protection for Oracle • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> • Instalación y actualización de Data Protection for VMware • Instalación de Data Protection for Microsoft Hyper-V

Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
 1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
 2. Pulse Más > Poner fuera de servicio.
- Para que un nodo cliente quede fuera de servicio utilizando un mandato administrativo, realice una de las siguientes acciones:
 - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
 - Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
 - Un valor null especifica que el nodo no está fuera de servicio.
 - Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

Proceso	Descripción proceso	Estado proceso
---------	---------------------	----------------

proceso		
3	DECOMMISSION NODE	Número de objetos de copia de seguridad desactivados para el nodo NODE1: 8 objetos desactivados.

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

Referencia relacionada:

- ➔ DECOMMISSION NODE (Poner fuera de servicio un nodo de cliente)
- ➔ DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

Referencia relacionada:

- ➔ DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

Gestión del almacenamiento de datos

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Auditoría de un contenedor de la agrupación de almacenamiento
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.
- Gestión de la capacidad de inventario
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- Gestión del uso de la memoria y del procesador
Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.
- Ajuste de actividades planificadas
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

Referencia relacionada:

- ➔ Tipos de agrupación de almacenamiento

Auditoría de un contenedor de la agrupación de almacenamiento

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.

Acerca de esta tarea

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

Procedimiento

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 000000000000076c.dcf:

```
audit container c:\tssm-storage\07\000000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

Qué hacer a continuación

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Emita el mandato AUDIT CONTAINER y especifique el nombre del contenedor.

Referencia relacionada:

- ➔ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- ➔ QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

Procedimiento

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
 - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
 - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.
- Sugerencias:
- El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.

- Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
 - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
 - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tabas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.
- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:
 Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
 1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
 2. Detenga el servidor.
 3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsiz 524288
```

- 4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
 5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

Referencia relacionada:

- ACTIVELOGSIZE, opción de servidor
- EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- SETOPT (Establecer una opción de servidor para actualización dinámica)

Gestión del uso de la memoria y del procesador

Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

Antes de empezar

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos admitidos para IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

Procedimiento

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

Procedimiento

1. Supervise el rendimiento de sistema de forma periódica para asegurarse de que las tareas de copia de seguridad y mantenimiento se completan correctamente. Para obtener más información sobre supervisión, consulte Supervisión de una solución de disco de sitio único.
2. Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, tal vez tenga que revisar la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
 - El número de clientes aumenta.
 - La cantidad de datos de los que se hace copia de seguridad aumenta.
 - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución tiene problemas de rendimiento. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
 - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
 - b. Pulse Detalles.
 - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos. Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.
4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:

- a. Copia de seguridad de la base de datos
- b. Ejecutar la caducidad para eliminar las copias de seguridad de cliente y las copias de archivo de archivado del almacenamiento de servidor.

Conceptos relacionados:

➔ Rendimiento

Tareas relacionadas:

➔ Deduplicación de datos (V7.1.1)

Protección del servidor IBM Spectrum Protect

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- **Conceptos sobre la seguridad**
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- **Gestión de administradores**
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.
- **Cambio de los requisitos de contraseña**
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- **Protección del servidor en el sistema**
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días. El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos de cliente	<ul style="list-style-type: none"> • REGISTER NODE • UPDATE NODE
Administradores	<ul style="list-style-type: none"> • REGISTER ADMIN • UPDATE ADMIN
Servidores	<ul style="list-style-type: none"> • DEFINE SERVER • UPDATE SERVER


Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

Tareas relacionadas:

 Protección de las comunicaciones

Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	<p>Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:</p> <ol style="list-style-type: none"> Registre el administrador y especifique Pa\$# \$twO como contraseña ejecutando el siguiente mandato: <pre>register admin admin1 Pa\$# \$twO</pre> Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre>
Cambie los permisos del administrador.	<p>Cambie el nivel de autorización de un administrador, ADMIN1.</p> <ul style="list-style-type: none"> Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <pre>revoke authority admin1 classes=system</pre>
Elimine administradores.	<p>Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect:</p> <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	<p>Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.</p>

Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, haga clic en el separador Propiedades.Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos. <p>El valor predeterminado en la instalación es 0.</p>
Establezca una longitud mínima para las contraseñas.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, pulse el separador Propiedades.Establezca el número de caracteres en el campo Longitud de contraseña mínima.
Establezca el periodo de caducidad para las contraseñas.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, pulse el separador Propiedades.Establecer el número de días en el campo Caducidad común de la contraseña.
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.</p> <p>Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

Conceptos relacionados:

- Autenticación de usuarios de IBM Spectrum Protect utilizando un servidor LDAP
- Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

Protección del servidor en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.
- Limitación de acceso a través de restricciones de puerto
Limitar acceso al servidor aplicando restricciones de puerto.

Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
 - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
 - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grabe en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique el parámetro BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Limitación de acceso a través de restricciones de puerto

Limitar acceso al servidor aplicando restricciones de puerto.

Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPPORT. Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPORT y SSLTCPPOINT.
SSLTCPPOINT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.

Opción de servidor	Acceso de puerto
SSLTCPADMINPORT	<p>Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.</p> <p>Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPSPORT y SSLTCPSPORT.</p>

Restricciones:

Las restricciones siguientes se aplican cuando especifica los puertos de servidor solo SSL (SSLTCPSPORT y SSLTCPADMINPORT):

- Cuando especifique el puerto de servidor solo SSL para LLADDRESS en el mandato DEFINE SERVER o el mandato UPDATE SERVER, debe especificar también el parámetro SSL=YES.
- Cuando especifique el puerto de servidor solo SSL para la opción TCPSPORT del cliente, debe especificar también YES para la opción del cliente SSL.

Referencia relacionada:

Planificación del acceso de cortafuegos

Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- **Inicio del servidor para tareas de mantenimiento o reconfiguración**
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Detención del servidor

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

Acerca de esta tarea

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

Procedimiento

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```
2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:
 - a. En la página Visión general del Centro de operaciones, vea el área Actividad para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.

- b. Vea el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:
 - El periodo actual, es decir, el periodo de 24 horas más reciente
 - El periodo anterior, es decir, 24 horas antes del periodo actualSi el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.
 - c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.
3. Espere hasta que las sesiones de nodo cliente se completen o cancélelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:
- En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
 - Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
 - Pulse Cancelar.
 - Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.
- Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.
4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Inicio del servidor para tareas de mantenimiento o reconfiguración

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, dmserv.opt, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

Procedimiento

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dmserv maintenance
```




Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

Qué hacer a continuación

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
 - o  Sistemas operativos AIX Inicio de la instancia de servidor
 - o  Sistemas operativos Linux Inicio de la instancia de servidor
 - o  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

Planificación para actualizar el servidor

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

Acerca de esta tarea

Siga estas directrices:




- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

Procedimiento

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

Qué hacer a continuación

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

Preparación para una parada o actualización de sistema

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

Acerca de esta tarea

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor.

Procedimiento

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
 - a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.

- b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
 - c. Pulse Cancelar.
2. Detenga el servidor emitiendo el mandato HALT:

halt

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

Implementación de un plan de recuperación tras desastre

Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

Acerca de esta tarea

Determine los requisitos que necesita para recuperación tras desastre identificando las prioridades empresariales respecto a la recuperación de nodo de cliente, los sistemas que utiliza para recuperar datos y si los nodos de cliente tienen conectividad con el servidor de recuperación. Utilice la réplica y la protección de agrupación de almacenamiento para proteger datos. También debe determinar la frecuencia con la que se protegen las agrupaciones de almacenamiento de contenedores de directorio.

- Realización de la obtención de detalles de recuperación
 - Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

Recuperación de paradas del sistema

Para soluciones de disco de sitio único de IBM Spectrum Protect, puede recuperar el inventario localmente únicamente y restaurar la base de datos para proteger los datos.

Procedimiento

Utilice uno de los métodos siguientes para recuperar el inventario para un sitio local, basado en el tipo de información del que se hace copia de seguridad.

Restricción: Puesto que las soluciones de disco de sitio único no tienen una segunda copia de la agrupación de almacenamiento, no puede restaurar las agrupaciones de almacenamiento. Para revisar la arquitectura de las soluciones de disco, consulte Selección de una solución de IBM Spectrum Protect.

Tabla 1. Escenarios para la recuperación tras un desastre

Escenario	Procedimiento
El sistema está inaccesible y desea restaurar localmente a una versión anterior utilizando las herramientas del sistema.	<ul style="list-style-type: none"> • Utilice IBM Spectrum Protect para hacer copia de seguridad del servidor a otro servidor. • Utilice las herramientas del sistema operativo para hacer copia de seguridad y restaurar el sistema a una versión anterior.

Escenario	Procedimiento
<p>Se ha producido una parada o desastre y desea restaurar datos desde las versiones de copia de seguridad de los datos.</p>	<ul style="list-style-type: none"> • Para hacer copia de seguridad de un cliente, en la página Clientes de TSM de Centro de operaciones, seleccione los clientes a los que desea hacer copia de seguridad y pulse Hacer copia de seguridad. • En la página Servidores de TSM de Centro de operaciones, seleccione el servidor de cuya base de datos desea hacer copia de seguridad. Pulse Copia de seguridad y siga las instrucciones que encontrará en la ventana Copia de seguridad de la base de datos del servidor. <p>Para restaurar una agrupación de almacenamiento de una versión de copia de seguridad de la agrupación de almacenamiento, debe restaurar la base de datos. Emita el mandato DSMSERV RESTORE DB para restaurar la base de datos y las agrupaciones de almacenamiento asociadas a una versión de copia de seguridad.</p>

- Restauración de la base de datos
Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

Referencia relacionada:

- ➔ [AUDIT CONTAINER](#) (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- ➔ [DSMSERV RESTORE DB](#) (Restaurar la base de datos)

Solución de disco multisitio

Esta solución de protección de datos proporciona réplica en varios sitios para que cada servidor proteja los datos del otro.

- Planificación de una solución de protección de datos de disco multisitio
Planifique una solución de protección de datos de disco multisitio con servidores en dos sitios que utilizan la deduplicación y la réplica de datos.
- Implementación de disco multisitio de una solución de protección de datos
La solución de disco multisitio se configura en dos sitios y utiliza la deduplicación y réplica de datos.
- Supervisión de una solución de disco multisitio
Después de implementar una solución de disco multisitio con IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.
- Gestión de operaciones para una solución de disco multisitio
Utilice esta información para gestionar operaciones para una solución de disco multisitio con IBM Spectrum Protect que incluye un servidor y utiliza la eliminación de datos duplicados para varias ubicaciones.

Planificación de una solución de protección de datos de disco multisitio

Planifique una solución de protección de datos de disco multisitio con servidores en dos sitios que utilizan la deduplicación y la réplica de datos.

Métodos de implementación

Puede configurar servidores para una solución de disco multisitio de las maneras siguientes:

Configure servidores utilizando los mandatos de Centro de operaciones y administrativos

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

Configure los servidores utilizando scripts automatizados

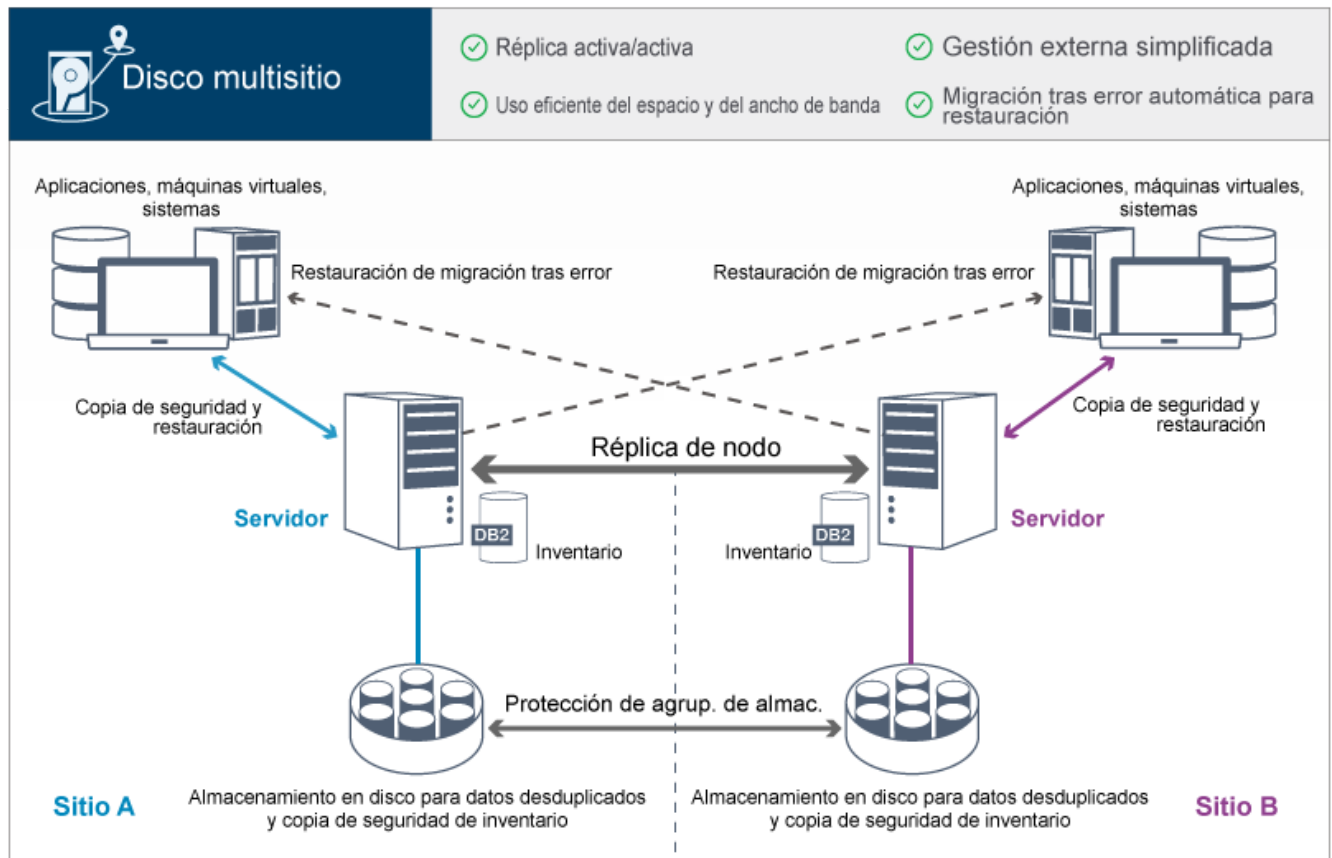
Para obtener instrucciones detalladas sobre la configuración con sistemas de almacenamiento de IBM® Storwize específicos y utilizando scripts automatizados para configurar cada servidor, consulte los blueprints de IBM Spectrum Protect. La documentación y los scripts están disponibles en IBM developerWorks en: IBM Spectrum Protect Blueprints.

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

Hoja de vía de acceso de planificación

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

Figura 1. Solución de disco multisitio



Los pasos siguientes son necesarios para planificar correctamente un entorno de disco multisitio.

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

Selección de un tamaño del sistema

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

Acerca de esta tarea

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

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

Tabla 1. Determinación del tamaño del servidor

Total de datos gestionados	Cantidad diaria de datos nuevos de los que se debe hacer copia de seguridad	Tamaño de servidor necesario
60 TB - 240 TB	Hasta 10 TB al día	Pequeño
196 TB - 784 TB	10 - 20 TB al día	Mediano
1000 TB - 4000 TB	20 - 100 TB al día	Grande

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

Planificación de los sitios

Revise los casos de uso y evalúe los factores para proporcionar la protección de datos más eficiente para la solución de disco multisitio para IBM Spectrum Protect.

Casos de uso

La solución de disco multisitio crea al menos una copia de los datos de copia de seguridad. Si los servidores de IBM Spectrum Protect están en ubicaciones independientes, la réplica de copia de seguridad se mantiene fuera del local.

Consejo: Evite los conflictos a la hora de gestionar los conjuntos de opciones de cliente y los ID administrativos identificando los ID y los conjuntos de opciones que se replicarán en el servidor de destino y los ID y conjuntos de opciones que se gestionarán en una configuración empresarial. No puede definir un ID de usuario administrativo para un nodo registrado si ya existe un ID administrativo en el mismo nodo.

Aunque su compañía puede beneficiarse de una solución de disco multisitio por diversos motivos, los motivos más comunes para utilizar una solución de disco multisitio incluyen los siguientes escenarios de réplica:

Réplica del sitio primario en el sitio de recuperación tras desastre

En este escenario, los datos de los que se hace una copia de seguridad desde el sitio primario, Sitio A, se replican en un servidor en el sitio secundario de recuperación tras desastre, sitio B. Si se produce un siniestro en el sitio A, como por ejemplo una anomalía del servidor, puede utilizar el servidor en el Sitio B para recuperar sistemas. De forma alternativa, puede utilizar el servidor en el Sitio A para restaurar los datos de agrupación de almacenamiento primario en el Sitio B, por ejemplo después de una anomalía de almacenamiento de disco en el Sitio B.

Réplica mutua en dos sitios activos

En este escenario, los servidores realizan la copia de seguridad de los datos locales de cada sitio tanto en el Sitio A como en el Sitio B. Los datos de los que se hace copia de seguridad desde el Sitio A se replican en el Sitio B y los datos de los que se ha hecho copia de seguridad desde el Sitio B se replican en el Sitio A. Si los datos de los que se ha hecho copia de seguridad se pierden en el Sitio A, puede utilizar el servidor en el Sitio B para recuperar los datos de agrupación de almacenamiento en el servidor en el Sitio A. Si el Sitio A ya no está disponible, puede recuperar los datos replicados para el Sitio A en un sistema nuevo del sitio B. Debe dimensionar los recursos de servidor para asegurarse de que ambos servidores tienen suficiente capacidad para realizar la copia de seguridad y la restauración de todos los nodos de cliente como parte del plan de recuperación tras desastre.

Proteger servidores remotos en el sitio primario

En este escenario, debe configurar servidores remotos que son relativamente pequeños para replicar los datos de copia de seguridad en un servidor más grande en el sitio primario. Si el ancho de banda es limitado, puede que no sea práctico restaurar sistemas en los sitios remotos. En este caso, es aconsejable recuperar sistemas en el sitio primario antes de replicar los datos de copia de seguridad en los servidores remotos.

Factores que deben evaluarse

Antes de implementar una solución de disco multisitio, evalúe los factores siguientes:

Ancho de banda de red

La red debe tener suficiente ancho de banda para las transferencias de datos esperadas entre nodos, para la réplica y para las operaciones de restauración entre sitios que son necesarias para la recuperación tras desastre. Antes de continuar con la prueba de rendimiento de réplica, asegúrese de que la red puede manejar el tráfico de réplica. Calcule el ancho de banda de red necesario para el requisito de estado estable aplicando las directrices de Estimación de ancho de banda de red necesario para la réplica (V7.1.1).

La conexión de red es con frecuencia un recurso compartido. Planee la hora del día para planificar la ejecución de la réplica de nodo a fin de evitar un conflicto con otros usuarios de recurso. Asimismo, los controles de red pueden limitar la actividad a sólo una parte del ancho de banda. No hay controles en IBM Spectrum Protect para restringir el uso de red.

Recursos para la réplica inicial

Para configurar la solución de protección de datos entre dos sitios, debe replicar los datos inicialmente del Sitio A en el servidor de destino del sitio B. Para garantizar que la réplica inicial se realiza correctamente, debe determinar si tiene el ancho de banda de red, los recursos de procesador y el tiempo disponible para replicar los datos. Es posible que tenga que planificar la réplica de las copias de seguridad completas iniciales a lo largo de varios días. Si no se puede ampliar la planificación para las copias de seguridad iniciales, puede replicar datos del Sitio A en el Sitio B sin utilizar la red. Por ejemplo, puede exportar e importar los datos de copia de seguridad utilizando soportes o temporalmente puede ubicar los servidores de origen y destino en el mismo sitio.

Ingestión de datos diaria

Para la solución de disco multisitio, la ingestión de datos diaria y la retención de datos total deben estar dentro de la capacidad de las configuraciones. Por ejemplo, una configuración grande tiene una capacidad de ingestión de datos de hasta 100 TB por día, incluida la réplica de nodos. En los casos en que los requisitos de copia de seguridad superan la capacidad de un solo servidor, puede configurar una solución que utilice varios servidores para alcanzar la capacidad necesaria.

Configuración del servidor

La configuración de servidor debe cumplir o superar los requisitos para la solución de disco multisitio.

Réplica única de datos de copia de seguridad

La solución de disco multisitio es más eficaz cuando una única copia fuera de sitio de los datos de copia de seguridad cumple los requisitos de protección de datos y mitigación de riesgos. En este caso, la única copia de los datos se mantiene fuera del local en la ubicación de un servidor de réplica.

Referencia relacionada:

Requisitos del sistema para una solución de disco multisitio


Requisitos del sistema para una solución de disco multisitio

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

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

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

Información relacionada:










 Sistemas operativos admitidos para IBM Spectrum Protect

Requisitos de hardware

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

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

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

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

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

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

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

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

Espacio de base de datos

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

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

Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 8 GB de espacio de registro de archivado cada 24 horas por cada 1000 clientes. En el ejemplo de 6500 clientes en el servidor concentrador y los servidores spoke, se utilizan 56 GB de espacio de registro de archivado a lo largo de un período de 24 horas para el servidor concentrador.

Para cada servidor de radio en el ejemplo, el espacio del registro de archivado que se utiliza a lo largo de 24 horas es aproximadamente 16 GB. Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en el requisito de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos:

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

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

Requisitos de hardware para el segundo servidor

Si tiene planificado configurar los sitios, de forma que todo lo del primer sitio se duplica en el segundo sitio, los requisitos de hardware son idénticos en ambos sitios. Si sólo desea replicar un subconjunto de datos para el segundo sitio, los requisitos de almacenamiento y red se pueden reducir.

Requisitos de software

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

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

Sistemas AIX

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

Sistemas Linux

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

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS
Otro software	Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado. Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: <ul style="list-style-type: none"> Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador

Tareas relacionadas:

🔗 Establecimiento de las opciones de red de AIX

Planificación de hojas de trabajo

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

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

Configuración previa de sistema servidor

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

Configuración del servidor

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

AIX

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

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

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

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 38 TB • Mediano: Al menos 180 TB • Grande: Al menos 500 TB 	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 10 sistemas de archivos • Mediano: Al menos 20 sistemas de archivos • Grande: Al menos 40 sistemas de archivos
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 3 TB • Mediano: Al menos 10 TB • Grande: Al menos 16 TB 	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 2 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6 <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

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

Elemento	Valor predeterminado	Valor	Notas
----------	----------------------	-------	-------

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 1 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p>

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

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 4.
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> • Pequeños y mediano: 140 GB • Grande: 300 GB 	
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> • Pequeño: 1 TB • Mediano: 2 TB • Grande: 4 TB 	
Directorios para la base de datos	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 1 TB • Mediano: Al menos 2 TB • Grande: Al menos 4 TB 	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 4 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 8 sistemas de archivos

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 38 TB • Mediano: Al menos 180 TB • Grande: Al menos 500 TB 	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 10 sistemas de archivos • Mediano: Al menos 20 sistemas de archivos • Grande: Al menos 40 sistemas de archivos
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 3 TB • Mediano: Al menos 10 TB • Grande: Al menos 16 TB 	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 2 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6 <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

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

Elemento	Valor predeterminado	Valor	Notas
----------	----------------------	-------	-------

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 3 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p>

Windows

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

Por ejemplo, C:\tsminst1\TSMdbspace00 es el punto de montaje para un volumen con su propio espacio. El volumen se correlaciona con un directorio bajo la unidad C:, pero no ocupa espacio de la unidad C:. La excepción es el directorio de instancia de servidor, C:\tsminst1, que puede ser un punto de montaje o un directorio normal.

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

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	C:\tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 6.
Directorio para el registro activo	C:\tsminst1\TSMalog		<ul style="list-style-type: none"> • Pequeños y mediano: 140 GB • Grande: 300 GB 	
Directorio para el registro de archivado	C:\tsminst1\TSMarchlog		<ul style="list-style-type: none"> • Pequeño: 1 TB • Medio: 2 TB • Grande: 4 TB 	
Directorios para la base de datos	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		Espacio total mínimo para todos los directorios: <ul style="list-style-type: none"> • Pequeño: Al menos 1 TB • Mediano: Al menos 2 TB • Grande: Al menos 4 TB 	Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema: <ul style="list-style-type: none"> • Pequeño: Al menos 4 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 8 sistemas de archivos

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para almacenamiento	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 38 TB • Mediano: Al menos 180 TB • Grande: Al menos 500 TB 	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 10 sistemas de archivos • Mediano: Al menos 20 sistemas de archivos • Grande: Al menos 40 sistemas de archivos
Directorios para la copia de seguridad de base de datos	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 3 TB • Mediano: Al menos 10 TB • Grande: Al menos 16 TB 	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> • Pequeño: Al menos 2 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6 <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

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

Elemento	Valor predeterminado	Valor	Notas
----------	----------------------	-------	-------

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 5 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	pAssW0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna. Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

Planificación de almacenamiento

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

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

hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

Base de datos y registro activo

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

Agrupación de almacenamiento

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

Referencia relacionada:

[Requisitos del sistema de almacenamiento y reducción del riesgo de corrupción de datos](#)

Planificación de la seguridad

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

Para obtener las directrices sobre la protección de entornos de almacenamiento ante ataques de ransomware y la recuperación de su entorno de almacenamiento en el caso de que se produzca un ataque, consulte Protección del entorno de almacenamiento ante ransomware.

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

Planificación de los roles de administración

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

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

Sistema

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

Política

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

Almacenamiento

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

Operador

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

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

Tabla 1. Escenarios para roles de administrador

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

Planificación para comunicaciones seguras

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

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

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

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

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

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

Tareas relacionadas:

[Protección de las comunicaciones](#)

Planificación de almacenamiento de datos cifrados

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

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

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

Información relacionada:

[Nota técnica 1963635](#)

Planificación del acceso de cortafuegos

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

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

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

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (TCPPOINT)	1500	Entrada/salida	Cada instancia de servidor necesita un puerto exclusivo. Puede especificar un número de puerto alternativo en lugar del predeterminado. La opción TCPPOINT realiza escuchas para sesiones habilitadas para TCP/IP y SSL desde el cliente. Para el tráfico de cliente administrativo, puede utilizar las opciones TCPADMINPORT y ADMINONCLIENTPORT para definir los valores de puerto.
Puerto solo SSL (SSLTCPPOINT)	No tiene valor predeterminado	Entrada/salida	Este puerto se utiliza si desea restringir la comunicación en el puerto a sesiones solo habilitadas para SSL. Para admitir tanto las comunicaciones SSL como las no SSL, utilice las opciones TCPPOINT o TCPADMINPORT.
SMB	45	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.
NDMP	No tiene valor predeterminado	Entrada/salida	<p>El servidor debe poder abrir una conexión de puerto de control NDMP de salida con el dispositivo NAS. El puerto de control de salida es la dirección de nivel inferior en la definición de transportador de datos para el dispositivo NAS.</p> <p>Durante una restauración NDMP de archivador a servidor, el servidor debe poder abrir una conexión de datos NDMP de salida con el dispositivo NAS. El puerto de conexión de datos que se utiliza durante una restauración puede configurarse en el dispositivo NAS.</p> <p>Durante las copias de seguridad NDMP de archivador a servidor, el dispositivo NAS debe poder abrir conexiones de datos de salida con el servidor y el servidor debe poder aceptar las conexiones de datos NDMP de entrada. Puede utilizar la opción de servidor NDMPPORTRANGE para restringir el conjunto de puertos disponibles para su uso como conexiones de datos NDMP. Puede configurar un cortafuegos para conexiones a estos puertos.</p>
Réplica	No tiene valor predeterminado	Entrada/salida	<p>El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica.</p> <p>Los puertos de entrada para la réplica son los puertos TCP y SSL que el servidor de origen indique en el mandato DEFINE SERVER.</p>
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesión de ejecución larga	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente-servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.

Elemento	Valor predeterminado	Dirección	Descripción
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	El puerto de servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

Implementación de disco multisitio de una solución de protección de datos

La solución de disco multisitio se configura en dos sitios y utiliza la deduplicación y réplica de datos.

Hoja de ruta de la implementación

Los pasos siguientes son necesarios para configurar un entorno de disco multisitio.

1. Configurar el sistema.
 - a. Configurar el hardware de almacenamiento y las matrices de almacenamiento para el tamaño del entorno.
 - b. Instalar el sistema operativo del servidor.
 - c. Configurar la E/S de multivía de acceso.
 - d. Crear el ID de usuario de la instancia de servidor.
 - e. Preparar sistemas de archivos para IBM Spectrum Protect.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
 - a. Completar la configuración inicial del servidor.
 - b. Configurar opciones de servidor.
 - c. Configurar la capa de sockets seguros del servidor y el cliente.
 - d. Configurar el Centro de operaciones.
 - e. Registrar la licencia de IBM Spectrum Protect.
 - f. Configurar la eliminación de duplicados de datos.
 - g. Definir las reglas de retención de datos para su empresa.
 - h. Definir programas de mantenimiento del servidor.
 - i. Definir programas de cliente.
4. Instalar y configurar clientes.
 - a. Registrar y asignar clientes a programas.
Consejo: Evite los conflictos a la hora de gestionar los conjuntos de opciones de cliente y los ID administrativos identificando los ID y los conjuntos de opciones que se replicarán en el servidor de destino y los ID y conjuntos de opciones que se gestionarán en una configuración empresarial. No puede definir un ID de usuario administrativo para un nodo registrado si ya existe un ID administrativo en el mismo nodo.
 - b. Instalar y verificar el servicio de gestión de clientes.
 - c. Configurar el Centro de operaciones para utilizar el servicio de gestión de clientes.
5. Configurar el segundo servidor.
 - a. Configuración de la comunicación de SSL entre el servidor central y el servidor spoke.
 - b. Añadir el segundo servidor como servidor spoke.
 - c. Habilitar la duplicación.
6. Completar la implementación.

Configuración del sistema

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

- Configuración del hardware de almacenamiento
Para configurar el hardware de almacenamiento, revise las directrices generales para los sistemas de disco y IBM Spectrum Protect.
- Instalación del sistema operativo del servidor
Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.
- Configuración de E/S de la multivía de acceso
puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

- Creación del ID de usuario para el servidor
Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.
- Preparación de sistemas de archivos para el servidor
Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

Configuración del hardware de almacenamiento

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

Procedimiento

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

Tareas relacionadas:

[Configuración del almacenamiento](#)

Instalación del sistema operativo del servidor

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

- Instalación en sistemas AIX
Complete los pasos siguientes para instalar AIX en el sistema servidor.
- Instalación en sistemas Linux
Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.
- Instalación en sistemas Windows
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

Instalación en sistemas AIX

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

Procedimiento

1. Instale AIX Versión 7.1, TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.
3. Abra el archivo /etc/hosts y complete las siguientes acciones:
 - Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:


```
192.0.2.7 server.yourdomain.com server
```
 - Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

mode	8023ad	
auto_recovery	yes	Habilitar la recuperación automática tras la migración tras error.
backup_adapter	NONE	Adaptador utilizado cuando falla todo el canal.
hash_mode	src_dst_port	Determina cómo se elige el adaptador saliente.
interval	long	Determina el valor de intervalo para IEEE.
mode	8023ad	Modalidad de 802.3ad
		Modalidad de funcionamiento de EtherChannel
netaddr	0	Dirección para el ping
no_loss_failover	yes	Habilitar migración tras error sin pérdidas tras anomalía del ping
num_retries	3	Veces que reintentar el ping antes de considerarlo un error
retry_time	1	Tiempo de espera (en segundos) entre pings
use_alt_addr	no	Habilitar dirección EtherChannel alternativa
use_jumbo_frame	no	Habilitar tramas de gran tamaño de Gigabit Ethernet

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

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

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	<i>ulimit -Hc</i>
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	<i>ulimit -Hd</i>
Tamaño de archivo máximo	fsize	Ilimitado	<i>ulimit -Hf</i>

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

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

Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.

Antes de empezar

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

Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
 - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
 - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
 - c. Seleccione las preferencias de idioma y teclado.
 - d. Seleccione la ubicación para establecer el huso horario correcto.
 - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
 - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:
 - El disco local de 300 GB se ha seleccionado como destino de instalación.
 - En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.

Pulse Terminado.
 - g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root. Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato `df` para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

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

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo. Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agregar varios puertos subordinados a una sola conexión lógica. El método preferido es utilizar una modalidad de vínculo de 802.3ad, un valor de `miimon` de 100 y un valor de `xmit_hash_policy` de `layer3+4`.

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

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

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:
 - Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

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

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

```
127.0.0.1 localhost
```

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

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

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

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

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

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

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

Si el directorio repos.d no existe, créelo.

- d. Liste el contenido de directorio:

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

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

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

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

```
vi rhel71_dvd.repo
```

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

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

- h. Instale el paquete de requisito previo ksh.x86_64, emitiendo el mandato yum. Por ejemplo:

```
yum install ksh.x86_64
```

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

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

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

```
umount /mnt
```

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

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

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

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

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

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

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

- a. Utilice el mandato sysctl -a para listar los valores de parámetro.
- b. Analice los resultados utilizando las directrices en Tabla 1 para determinar si es necesario algún cambio.
- c. Si se necesitan cambios, establezca los parámetros en el archivo /etc/sysctl.conf. Los cambios de archivo se aplican cuando se inicia el sistema.

Consejo: Ajuste automáticamente los valores de parámetros de kernel y elimine la necesidad de actualizaciones manuales en estos valores. En Linux, el software de base de datos DB2 ajusta automáticamente los valores del parámetro de kernel de

comunicación entre procesos (IPC) a los valores preferidos. Para obtener más información sobre los valores de parámetros de kernel, busque los parámetros de kernel de Linux en Documentación del producto IBM DB2 Versión 11.1.

Tabla 1. Valores óptimos del parámetro de kernel Linux

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

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

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

Emita el mandato siguiente:

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

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

Emita el mandato siguiente:

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

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

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

Emita el mandato siguiente:

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

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

Emita el mandato siguiente:

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

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

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

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

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

Instalación en sistemas Windows

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

Procedimiento

1. Instale Windows Server 2016 Standard Edition, de acuerdo con las instrucciones del fabricante.
2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
 - a. Abra el editor de política de seguridad local ejecutando `secpol.msc`.
 - b. Pulse Políticas locales > Opciones de seguridad y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
 - Modo de aprobación de administrador para la cuenta de administrador integrado
 - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:
 - a. Aplique las últimas actualizaciones de Windows Server 2016.
 - b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
 - c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
 - d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.
5. Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato:

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

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

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

Configuración de E/S de la multivía de acceso

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

- Sistemas AIX
- Sistemas Linux
- Sistemas Windows

Sistemas AIX

Procedimiento

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

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

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
```

- En sistemas grandes, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
lscfg -vps -l fcs2 | grep "Network Address"
lscfg -vps -l fcs3 | grep "Network Address"
```

2. Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:

- `devices.common.IBM.mpio.rte`
- `devices.fcp.disk.array.rte`
- `devices.fcp.disk.rte`

3. Emita el mandato `cfgmgr` para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

4. Para listar los discos disponibles, emita el siguiente mandato:

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Utilice la salida del mandato `lsdev` para identificar y listar ID de dispositivo para cada dispositivo de disco.

Por ejemplo, un ID de dispositivo podría ser `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

```
lspv -u
```

En un sistema IBM® Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

```
hdisk4 00f8cf083fd97327 None active
3321360050763008101057800000000000003004214503IBMfcp
```

En el ejemplo, `6005076300810105780000000000030` es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

Para verificar el tamaño de disco en megabytes y compararlo con el valor que se lista para el sistema, emita el siguiente mandato:

```
bootinfo -s hdisk4
```

Procedimiento

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

```
mpathconf --enable
```

Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los mandatos siguientes:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

```
multipath -l
```

4. Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan.
Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

```
[root@tapsrv01 code]# multipath -l
36005076802810c50980000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  `-- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  `-- 3:0:0:18 sddy 128:0 active undef running
```

- a. Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

```
echo "-- --" > /sys/class/scsi_host/host0/scan
echo "-- --" > /sys/class/scsi_host/host1/scan
echo "-- --" > /sys/class/scsi_host/host2/scan
```

También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

- b. Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato `multipath -l`.

5. Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es `36005076802810c50980000000000012`.

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

Sistemas Windows

Procedimiento

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
2. Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan. Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

```
DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0
```

4. Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 60050763008101057800000000000034

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

5. Para poner los nuevos discos en línea y borrar el atributo de 'sólo lectura', ejecute diskpart.exe con los mandatos siguientes. Repítalo para cada uno de los discos:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

Creación del ID de usuario para el servidor



Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.

Acerca de esta tarea

Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado (_) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Procedimiento

1. Utilice mandatos del sistema operativo para crear un ID de usuario.
 -  Sistemas operativos AIX  Sistemas operativos Linux Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

Por ejemplo, para crear el ID de usuario `tsminst1` en el grupo `tsmsrvrs` con una contraseña de `tsminst1`, emita los siguientes mandatos desde un ID de usuario de administración:


Sistemas operativos AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

Sistemas operativos Linux

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

- o  Sistemas operativos Windows Cree un ID de usuario y, a continuación, añada el nuevo ID al grupo de administradores. Por ejemplo, para crear el ID de usuario `tsminst1`, emita el siguiente mandato:

```
net user tsminst1 * /add
```

Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Cierre la sesión con el nuevo ID de usuario.

Preparación de sistemas de archivos para el servidor

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

- Preparación de sistemas de archivos en sistemas AIX
Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.
- Preparación de sistemas de archivos en sistemas Linux
Debe formatear los sistemas de archivos `ext4` o `xf`s en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.
- Preparación de sistemas de archivos en sistemas Windows
Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Preparación de sistemas de archivos en sistemas AIX

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

Procedimiento

1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos `hdiskX` disponibles. Emita los siguientes mandatos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, `hdisk0`.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato `mkvg`, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

Por ejemplo, si los nombres de dispositivo `hdisk4`, `hdisk5` y `hdisk6` corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```

mkvlg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvlg -S -y tsmactlog hdisk5
mkvlg -S -y tsmarchlog hdisk6
mkvlg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvlg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49

```

- Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita lsvg para cada grupo de volúmenes que ha creado en el paso anterior.

Por ejemplo:

```
lsvg -p tsmdb
```

La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

```

tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631       1631      327..326..326..326..326
hdisk5   active    1631       1631      327..326..326..326..326
hdisk6   active    1631       1631      327..326..326..326..326

```

- Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato mklv. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco. Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

```

mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4

```

- De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato crfs.

Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

```

crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes

```

- Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

```
mount -a
```

- Liste todos los sistemas de archivos emitiendo el mandato df. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado es normalmente un 1%:

```

tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks  Free      %Used    Iused     %Iused    Mounted on
/dev/tsmact00   195.12    194.59    1%        4         1%        /tsminst1/TSMalog

```

- Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios para el servidor IBM Spectrum Protect.

Preparación de sistemas de archivos en sistemas Linux

Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

- Utilizando la lista de ID de dispositivo que ha generado antes, emita el mandato mkfs para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos xfs:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Puede emitir el mandato mkfs hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

2. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato `mkdir` para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación.

Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
mkdir /tsminst1
```

Repita el mandato `mkdir` para cada sistema de archivos.

3. Añada una entrada en el archivo `/etc/fstab` para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.

Por ejemplo:

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Monte los sistemas de archivos que ha añadido al archivo `/etc/fstab` emitiendo el mandato `mount -a`.
5. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente en un sistema IBM® Storwize muestra que la cantidad de espacio utilizado normalmente es un 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%  /tsminst1/TSMalog
```

6. Compruebe que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura a los directorios de IBM Spectrum Protect.

Preparación de sistemas de archivos en sistemas Windows

Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

1. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato `md` para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
md c:\tsminst1
```

Repita el mandato `md` para cada sistema de archivos.

2. Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

Vaya a Gestor de servidores > Servicios de archivo y almacenamiento y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

- a. Ponga el disco en línea.
- b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
- c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como `TSMfile00`. No asigne el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como `C:\tsminst1\TSMfile00`.

Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.

3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato `mountvol` y, a continuación, revise la salida. Por ejemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
C:\tsminst1\TSMdbspace00\
```

4. Una vez se ha completado la configuración de disco, reinicie el sistema.

Qué hacer a continuación

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

Instalación del servidor y Centro de operaciones

Utilice el asistente gráfico de IBM® Installation Manager para instalar los componentes.

- Instalación en sistemas AIX y Linux
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema de servidor.
- Instalación en sistemas Windows
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema servidor.


Instalación en sistemas AIX y Linux

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema de servidor.

Antes de empezar

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

Procedimiento


1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.
Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.
2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package_name* es el nombre del archivo descargado.

6.  Sistemas operativos AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:

```
lsuser
```

De manera predeterminada, el mandato está habilitado.

7. Cambie al directorio en el que colocó el archivo ejecutable.
8. Inicie el asistente de instalación emitiendo el mandato siguiente:

```
./install.sh
```

Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.
- Instalación de archivos RPM de requisitos previos para el asistente gráfico
Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

Tareas relacionadas:

- 📄 Otros métodos para instalar componentes de IBM Spectrum Protect (AIX)
- 📄 Otros métodos para instalar componentes de IBM Spectrum Protect (Linux)

Instalación en sistemas Windows

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema servidor.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

Procedimiento

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM®.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.

Tareas relacionadas:

- 📄 Otros métodos para instalar componentes de IBM Spectrum Protect

Configuración del servidor y el Centro de operaciones

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

- Configuración de la instancia de servidor
Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.
- Instalación del cliente de archivado y copia de seguridad
Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?
- Configuración de opciones para el servidor
Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.
- Configuración de comunicaciones seguras con Seguridad de la capa de transporte
Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.
- Configuración de Centro de operaciones
Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.
- Registro de la licencia de producto
Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.

- Configuración de la optimización de almacenamiento de datos
Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.
- Definición de las reglas de retención de datos para su empresa
Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.
- Definición de planificaciones para actividades de mantenimiento del servidor
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.
- Definición de planificaciones de cliente
Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

Configuración de la instancia de servidor

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

 Sistemas operativos Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:




1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
 - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
 - b. Seleccione Configuración avanzada.
 - c. Seleccione Reglas de entrada.
 - d. Seleccione Nueva regla.
 - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
 - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
 - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
 - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
 - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada > Inhabilitar > Aceptar.
4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.



Acerca de esta tarea


El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

Procedimiento

1. Inicie la versión local del asistente.

-   Abra el programa dsmsicfgx en el directorio /opt/tivoli/tsm/server/bin. Este asistente sólo puede ejecutarse como usuario root.
 -  Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Planificación de hojas de trabajo para la configuración del sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.

  En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.

 Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo dsmserv.opt.
2. Revise los valores de la tabla siguiente y verifique los valores de opciones de servidor, en base al tamaño del sistema.

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Sí	No	No
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo dsmserv.opt y utilice el mandato SETOPT desde la interfaz de línea de mandatos de administración para establecer las opciones.

Por ejemplo, para actualizar la opción IDLETIMEOUT a 60, emita el siguiente mandato:

```
setopt idletimeout 60
```

3. Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

Opción de servidor	Todos los tamaños del sistema
SSLFIPSMODE	NO
TCPPOINT	Especifique el número de puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente.
TCPADMINPORT	Especifique la dirección del puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente administrativo de línea de mandatos.

Si alguno de los valores de opción debe actualizarse, edite el archivo dsmserv.opt utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guarde los cambios y cierre el archivo. Si edita el archivo dsmserv.opt directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

Referencia relacionada:

- ➔ Referencia de opciones de servidor
- ➔ SETOPT (Establecer una opción de servidor para actualización dinámica)

Configuración de comunicaciones seguras con Seguridad de la capa de transporte

Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

Acerca de esta tarea

A partir de IBM Spectrum Protect versión 8.1.2, SSL está habilitada de forma predeterminada, y el servidor y cliente de archivado y copia de seguridad de IBM Spectrum Protect se configuran automáticamente para comunicarse entre ellos utilizando el protocolo TLS 1.2.

Tal como se indica en la figura siguiente, puede configurar manualmente comunicaciones seguras entre el servidor y el cliente de archivado y copia de seguridad definiendo opciones en los archivos de opciones de servidor y cliente y, después, transfiriendo el certificado firmado automáticamente que se ha generado en el servidor al cliente. Como alternativa, puede obtener y transferir un certificado único que esté firmado por una entidad emisora de certificados (CA).



Para obtener más información sobre cómo configurar el servidor y los clientes para las comunicaciones SSL o TLS, consulte Configuración de agentes, servidores y clientes de almacenamiento, y del Centro de operaciones para conectarse al servidor mediante SSL.

Configuración de Centro de operaciones

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

Antes de empezar

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

Procedimiento

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

```
https://hostname:secure_port/oc
```

donde:

- *nombre_host* representa el nombre del sistema donde está instalado Centro de operaciones
- *puerto_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

Por ejemplo, si el nombre de host es `tsm.storage.mylocation.com` y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

```
https://tsm.storage.mylocation.com:11090/oc
```

Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.

2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor concentrador configurando el protocolo de la capa de sockets seguros (SSL).

Siga las instrucciones que encontrará en Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

Siga las instrucciones que encontrará en Seguimiento del estado del sistema mediante informes de correo electrónico.

- Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador
Para proteger las comunicaciones entre Centro de operaciones y el servidor concentrador, añada el certificado de seguridad de la capa de transporte (TLS) del servidor concentrador al archivo de almacén de confianza de Centro de operaciones.

Registro de la licencia de producto


Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.

Acerca de esta tarea

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

Procedimiento


Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.

1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración  y pulsando Creador de mandatos.
3. Emita el mandato REGISTER LICENSE. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

Qué hacer a continuación

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor se ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
-  Sistemas operativos Linux Si cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

Referencia relacionada:

 REGISTER LICENSE (Registrar una nueva licencia)

Configuración de la optimización de almacenamiento de datos

Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.

Antes de empezar

Utilice la información de directorio de agrupación de almacenamiento que ha registrado en Planificación de hojas de trabajo para esta tarea.

Procedimiento

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el cursor por encima de Almacenamiento.
3. En la lista que se visualiza, pulse Agrupaciones de almacenamiento.
4. Pulse el botón +Agrupación de almacenamiento.
5. Complete los pasos del asistente Añadir agrupación de almacenamiento:
 - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
 - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
6. Tras configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.

Definición de las reglas de retención de datos para su empresa

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.
3. Pulse el conmutador Configurar y realice los cambios siguientes:
 - Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedores de directorio.
 - Cambie el valor de la columna de copias de seguridad a Sin límite.
 - Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador Configurar para que el conjunto de políticas ya no se pueda editar.
5. Activar el conjunto de políticas pulsando Activar.

Tareas relacionadas:

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

Definición de planificaciones para actividades de mantenimiento del servidor

Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.

Acerca de esta tarea

Planifique operaciones de mantenimiento de servidor para ejecutar después de operaciones de copia de seguridad de cliente. Puede controlar la temporización de planificaciones estableciendo la hora de inicio en combinación con la duración para cada operación.

El ejemplo siguiente muestra cómo puede planificar procesos de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de disco multisitio.

Operación	Planificación
Copia de seguridad del cliente	Empieza a las 22:00.
Réplica de nodo	Se inicia a las 08:00, o 10 horas después del comienzo de la copia de seguridad de cliente.
Proceso para archivos de recuperación tras desastre y de base de datos	<ul style="list-style-type: none">La copia de seguridad de base de datos se inicia a las 11:00, o 13 horas después del comienzo de la copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 17:00 o 6 horas después del inicio de la copia de seguridad de la base de datos.La supresión del historial de volumen comienza a las 20:00 o 9 horas después del inicio de la copia de seguridad de la base de datos.
Caducidad de inventario	Empieza a las 12:00, o 14 horas después del inicio de la ventana de copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.



Procedimiento

Tras configurar la clase de dispositivo para las operaciones de copia de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato DEFINE SCHEDULE. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.


1. Defina una clase de dispositivo para las operaciones de copia de seguridad. Por ejemplo, utilice el mandato DEFINE DEVCLASS para crear una clase de dispositivo que se denomine DBBACK_FILEDEV:

```
define devclass dbback_filedev devtype=file
  directory=directorios_copia_seguridad_bd
```

donde *directorios_copia_seguridad_bd* es una lista de los directorios que ha creado para la copia de seguridad de base de datos.

 Sistemas operativos AIX  Sistemas operativos Linux Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando por el mandato /tsminst1/TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

 Sistemas operativos Windows Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando con C:\tsminst1\TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

2. Establezca la clase de dispositivo para operaciones de copia de seguridad de base de datos automáticas. Utilice el mandato SET DBRECOVERY para especificar la clase de dispositivo que ha creado en el paso anterior. Por ejemplo, si la clase de dispositivo es dbback_filedev, emita el mandato siguiente:

```
set dbrecovery dbback_filedev
```

3. Cree planificaciones para las operaciones de mantenimiento utilizando el mandato DEFINE SCHEDULE. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.
Consejo: Cree la planificación para la réplica por separado en un paso posterior, al utilizar Centro de operaciones para configurar la réplica.

Operación	Mandato de ejemplo
Realizar una copia de seguridad de la base de datos.	<p>Cree una planificación para ejecutar el mandato BACKUP DB. Si está configurando un sistema pequeño, establezca el parámetro COMPRESS en YES.</p> <p>Por ejemplo, en un sistema pequeño, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes</pre>
Realice una copia de seguridad de la información de configuración del dispositivo.	<p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
Haga una copia de seguridad del historial de volumen.	<p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	<p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>
Elimine objetos que exceden su retención permitida.	<p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY. Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar:</p> <ul style="list-style-type: none"> o Sistemas pequeños: 10 o Sistemas medianos: 30 o Sistemas grandes: 40 <p>Por ejemplo, en un sistema de tamaño mediano, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes</pre>

Qué hacer a continuación

Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Servidores.
2. Pulse Mantenimiento.

Referencia relacionada:

➔ DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

Definición de planificaciones de cliente

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

Procedimiento

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de Clientes.
2. Pulse Planificaciones.
3. Pulse +Planificación.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.

Instalación y configuración de clientes de archivado y copia de seguridad

Tras la configuración correcta del sistema servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

Qué hacer a continuación

Registrar y asignar los clientes a planificaciones.

- Registro y asignación de clientes a planificaciones
Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.
- Instalación del servicio de gestión de cliente
Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

Registro y asignación de clientes a planificaciones

Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.

Antes de empezar

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
 - a. En la barra de menús de Centro de operaciones, pulse Clientes.
 - b. En la tabla Clientes, pulse + Cliente.
 - c. Complete los pasos en el asistente Añadir cliente:
 - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
 - ii. En la ventana Configuración, copie los valores de opción TCPSERVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
 - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
 - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
 - v. Pulse Añadir cliente.

Instalación del servicio de gestión de cliente

Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

Procedimiento

Instale el servicio de gestión de cliente en el mismo sistema que el cliente de archivado y copia de seguridad completando los pasos siguientes:

1. Descargue el paquete de instalación para el servicio de gestión de cliente desde un sitio de descarga de IBM® como por ejemplo IBM Passport Advantage® o IBM Fix Central. Busque un nombre de archivo que sea similar a `<versión>-IBM_Spectrum_Protect-CMS-sistema_operativo.bin`.
 2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
 3. Extraiga el contenido del archivo del paquete de instalación.
 4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
 5. Para instalar el servicio de gestión de cliente, siga las instrucciones del asistente del Gestor de instalación de IBM. Si el Gestor de instalación de IBM no está instalado en el sistema cliente, debe seleccionar el Gestor de instalación de IBM y los Servicios de gestión de cliente de IBM Spectrum Protect.
- Verificación de que el servicio de gestión de clientes está instalado correctamente
Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.
 - Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente
Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

Tareas relacionadas:

- 🔗 Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas

Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.

Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

```
dir_instalación_cliente/cms/bin/CmsConfig.sh list
```

donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

  Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252

  Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

- En los sistemas cliente Windows, emita el mandato siguiente:

```
dir_instalación_cliente\cms\bin\CmsConfig.bat list
```

donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
C:\Archivos de programa\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252

  Log File: C:\Program Files\Tivoli\TSM\baclient\dsm Sched.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo *client-configuration.xml*. Para obtener instrucciones para configurar este archivo, consulte Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato *CmsConfig verify* para comprobar que una definición de nodo se ha creado correctamente en el archivo *client-configuration.xml*.

Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente

Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

Antes de empezar

Asegúrese de que el servicio de gestión de cliente está instalado y se ha iniciado en el sistema cliente. Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de cliente no utiliza el número de puerto predeterminado, 9028.

- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
 - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse por una red, mientras que el servicio de gestión de cliente se comunica por la otra red.
 - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, se le asigna dinámicamente al sistema cliente una dirección IP, que se guarda en el servidor durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

Procedimiento

Para configurar Centro de operaciones para utilizar el servicio de gestión de cliente, complete los pasos siguientes:

1. En la página Clientes de Centro de operaciones, seleccione el cliente.
2. Pulse Detalles > Propiedades.
3. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de cliente en el sistema cliente. La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	<code>https://server.example.com</code>
Con el nombre de host de DNS y puerto no predeterminado	<code>https://server.example.com:1599</code>
Con la dirección IP y puerto no predeterminado	<code>https://192.0.2.0:1599</code>

4. Pulse Guardar.

Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

Configuración del segundo servidor

Después de completar la configuración para el primer servidor del sistema, configure el segundo servidor.

Procedimiento

Complete las instrucciones de las secciones siguientes:

1. Para configurar un segundo servidor que sea igual que el primer servidor, complete las instrucciones de las secciones siguientes:
 - a. Configuración del sistema
 - b. Instalación del servidor y Centro de operaciones

Sólo un servidor de la solución de disco multisitio está configurada como el servidor concentrador, de modo que no necesita instalar el Centro de operaciones en el segundo servidor. Cuando seleccione los paquetes de instalación para instalar en el segundo servidor, no seleccione el Centro de operaciones.
 - c. Configuración del servidor y el Centro de operaciones

Sáltese las tareas para configurar el Centro de operaciones.
 - d. Instalación y configuración de clientes de archivado y copia de seguridad
2. Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke
3. Añadir un segundo servidor como servidor spoke
4. Habilitación de réplica

Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke

Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke utilizando el protocolo de Seguridad de la capa de transporte (TLS), debe definir el certificado del servidor spoke en el servidor concentrador.

Acerca de esta tarea

El servidor concentrador recibe información de alerta y estado del servidor de radio y muestra esta información en el Centro de operaciones. Para recibir información de estado y de alerta del servidor spoke, debe añadirse el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador. También debe configurar Centro de operaciones para supervisar el servidor spoke.

Para habilitar otras funciones del Centro de operaciones, como el despliegue automático de actualizaciones del cliente, el certificado del servidor concentrador debe añadirse al archivo de almacén de confianza del servidor spoke.

Procedimiento

1. Realice los pasos siguientes para definir el certificado del servidor de radio en el servidor concentrador:

- En el servidor spoke, cambie al directorio de la instancia del servidor spoke.
- Especifique el certificado cert256.arm necesario como certificado predeterminado en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

- Verifique los certificados en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- Transfiera de forma el archivo cert256.arm del servidor de radio al servidor central.
- En el servidor concentrador, cambie el directorio de la instancia del servidor concentrador.
- Defina el certificado de servidor spoke para el servidor concentrador. Emita el mandato siguiente desde el directorio de instancia de servidor concentrador, donde *nombre_servidor_spoke* es el nombre del servidor spoke y *spoke_cert256.arm* es el nombre de archivo del certificado de servidor spoke.

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label spoke_servername -file spoke_cert256.arm
```

2. Realice los pasos siguientes para definir el certificado del servidor concentrador en el servidor de radio:

- En el servidor concentrador, cambie el directorio de la instancia del servidor concentrador.
- Especifique el certificado cert256.arm necesario como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

- Verifique los certificados en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- Transfiera de forma el archivo cert256.arm del servidor concentrador al servidor de radio.
- En el servidor spoke, cambie al directorio de la instancia del servidor spoke.
- Defina el certificado del servidor concentrador hub en el servidor de radio. Emita el siguiente mandato desde el directorio de la instancia del servidor de radio, donde *nombre_servidor_concentrador* es el nombre del servidor concentrador y *hub_cert256.arm* es el nombre de archivo del certificado del servidor concentrador:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label nombre_servidor_concentrador -file hub_cert256.arm
```

3. Reinicie el servidor central y el servidor de radio.

4. Realice los pasos siguientes para definir el servidor de radio para el servidor concentrador, y el servidor concentrador para el servidor de radio.

- Emita los mandatos siguientes tanto en el servidor concentrador como en el servidor de radio:

```
SET SERVERPASSWORD contraseña_servidor  
SET SERVERHLADDRESS dirección_ip  
SET SERVERLLADDRESS puerto_tcp
```

- En el servidor concentrador, emita el mandato DEFINE SERVER, de acuerdo con el ejemplo siguiente:

```
DEFINE SERVER spoke_servername HLA=spoke_address  
LLA=spoke_SSLTCPADMINPort SERVERPA=contraseña_servidorespoke
```



- En el servidor de radio, emita el mandato DEFINE SERVER, de acuerdo con el ejemplo siguiente:

```
DEFINE SERVER nombre_servidor_concentrador HLA=dirección_concentrador  
LLA=hub_SSLTCPADMINPort SERVERPA=contraseña_servidor_concentrador
```

Consejo: De manera predeterminada la comunicación del servidor se cifra, excepto cuando el servidor está enviando o recibiendo datos de objeto. Los datos de objeto se envían y reciben mediante TCP/IP. Al elegir no cifrar los datos, el rendimiento del servidor es similar al de la comunicación por una sesión TCP/IP y la sesión es segura. Para cifrar toda la comunicación con el servidor especificado, incluso cuando el servidor está enviando y recibiendo datos de objeto, especifique el parámetro SSL=YES en el mandato DEFINE SERVER.

5. Realice los pasos siguientes para configurar el Centro de operaciones para supervisar el servidor de radio:
 - a. En la barra de menús de Centro de operaciones, pulse Servidores. El servidor de radio tiene el estado "No supervisado". Este estado significa que, aunque se haya definido este servidor en el servidor concentrador utilizando el mandato DEFINE SERVER, el servidor aún no está configurado como servidor de radio.
 - b. Pulse el servidor de radio (spoke) para resaltar el elemento y pulse Supervisar radio.

Referencia relacionada:

-  DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)
-  QUERY OPTION (Consultar opciones del servidor)

Añadir un segundo servidor como servidor spoke

Después de configurar ambos servidores en el entorno, añada el segundo servidor como servidor spoke al servidor concentrador.

Procedimiento

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pulse Servidores.
3. Realice uno de los siguientes pasos:
 - o Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
 - o Si el servidor que desea añadir no se muestra en la tabla, pulse +Spoke.
4. Realice los pasos del asistente de configuración de spoke.

Habilitación de réplica

Para proteger los datos, habilite la réplica de nodo, además de proteger las agrupaciones de almacenamiento.

Procedimiento

Para habilitar la réplica de nodo para todos los clientes registrados para el servidor de origen, complete los pasos siguientes:

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
3. En la página Réplica, pulse + Par de servidores.
4. Realice los pasos del asistente Añadir par de servidores:
 - o Establezca el servidor de origen como el primer servidor que ha configurado para la solución de disco multisitio. El servidor de destino es el segundo servidor.
 - o Establezca que la planificación de réplica de nodo se inicie 10 horas después de la ventana de copia de seguridad de cliente, basándose en las actividades de mantenimiento de servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.
 - o El asistente configura planificaciones de protección de agrupación de almacenamiento, en función de la cantidad de datos que se están protegiendo y de cuándo se planifica la réplica de cliente.

Qué hacer a continuación

Si piensa configurar la réplica mutua entre dos sitios, ejecute el asistente Añadir par de servidores de nuevo y establezca el segundo servidor como el origen y el primer servidor como el destino.

Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

Procedimiento

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
 - a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
 - b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
 - c. Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.
Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.
2. Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de disco multisitio.

Supervisión de una solución de disco multisitio

Después de implementar una solución de disco multisitio con IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

Acerca de esta tarea

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar un informe de correo electrónico diario que resume el estado del sistema.

En algunos casos, es posible que desee utilizar herramientas de supervisión avanzadas para completar tareas de supervisión o resolución de problemas específicas.

Consejo: Si piensa diagnosticar problemas con clientes de archivado y copia de seguridad en sistemas operativos Linux o Windows, instale los servicios de gestión de cliente de IBM Spectrum Protect en cada sistema donde esté instalado un cliente de archivado y copia de seguridad. De esta forma, puede garantizar que el botón Diagnosticar está disponible en Centro de operaciones para diagnosticar problemas con los clientes de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.

Procedimiento

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación de supervisión diaria.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación de supervisión periódica.
3. Para verificar que la solución de IBM Spectrum Protect cumple con los requisitos de licencia, siga las instrucciones que encontrará en Verificación de la conformidad de licencia.
4. Si desea configurar el Centro de operaciones para generar informes de estado de correo electrónico, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

Qué hacer a continuación

Resuelva cualquier problema que encuentre. Para resolver un problema cambiando la configuración de la solución, siga las instrucciones que encontrará en Gestión de operaciones para una solución de disco multisitio. Los siguientes recursos están también disponibles:

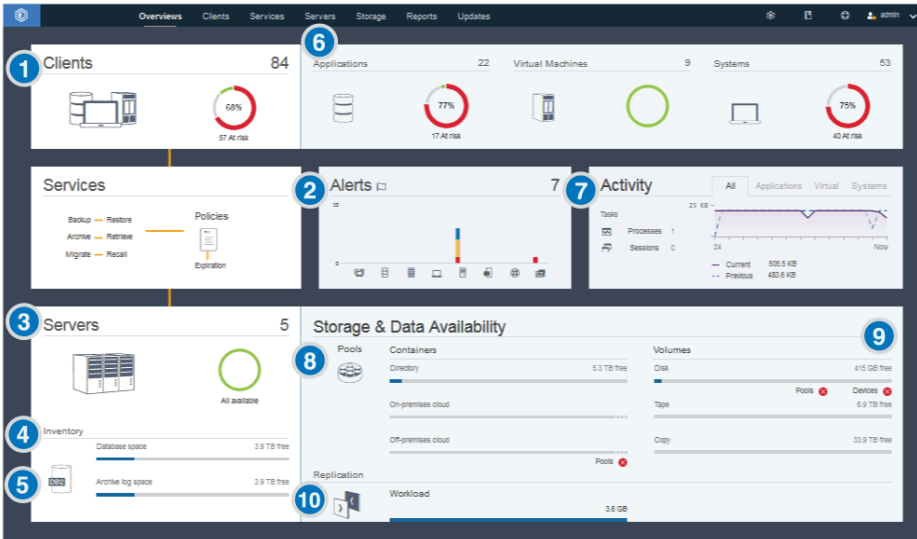
- Para resolver problemas de rendimiento, consulte Rendimiento.
- Para resolver otros tipos de problemas, consulte Resolución de problemas.


Lista de comprobación de supervisión diaria

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.









Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.



Tabla 1. Tareas de supervisión diarias



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>1 Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Atención: Si el porcentaje En riesgo es superior al habitual, es posible que indique que se ha producido un ataque de ransomware. Un ataque de ransomware puede hacer que las operaciones de copia de seguridad fallen, poniendo a los clientes en una situación de riesgo. Por ejemplo, si el porcentaje de clientes en riesgo se encuentra habitualmente entre un 5% y un 10%, pero el porcentaje se incrementa a un 40% o 50%, investigue la causa. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Clientes, seleccione el cliente y pulse Detalles. 2. Para diagnosticar un problema, pulse Diagnóstico. 	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>
<p>2 Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Alertas. 2. En la tabla Alertas, seleccione una alerta. 3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.


Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>3 Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> 1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible. 2. Para ver información adicional, pulse el área Servidores. 3. Seleccione un servidor en la tabla Servidores y pulse Detalles. 	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione un servidor y pulse Detalles. 2. Para actualizar las propiedades de servidor, pulse Propiedades.
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado. o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor. o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio. o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC. o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio. 	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>5 Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos. 	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione una fila y pulse Detalles. 2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad. <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Servidores. 2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad. <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Emita el mandato QUERY DB: <pre>query db f=d</pre> 3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.
<p>6 Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse Servidores > Mantenimiento. 2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial. 3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso. 	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>7 Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> • Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad. • Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores. 	<ul style="list-style-type: none"> • Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente. Atención: Si la cantidad de datos de copia de seguridad es significativamente superior a lo habitual, puede que indique un ataque de ransomware. Cuando un ransomware cifra datos, el sistema percibe que se están cambiando los datos, y realiza una copia de seguridad de los datos cambiados. Así, los volúmenes de copia de seguridad se vuelven más grandes. Para determinar qué clientes están afectados, pulse los separadores Aplicaciones, Virtual o Sistemas. • Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>8 Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<p>1. Si se indican problemas en el área Almacenamiento & Disponibilidad de datos, pulse Agrupaciones para ver los detalles:</p> <ul style="list-style-type: none"> ○ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible. Atención: Si el estado es crítico, investigue la causa: <ul style="list-style-type: none"> ■ Si el índice de deduplicación de datos para una agrupación de almacenamiento cae significativamente, puede indicar un ataque de ransomware. Durante un ataque de ransomware, se cifran los datos y estos no podrán ser deduplicados. Para verificar el índice de deduplicación de datos, en la tabla Agrupaciones de almacenamiento, revise el valor de la columna % de ahorro. ■ Si la agrupación de almacenamiento muestra inesperadamente un uso del 100%, esto puede indicar un ataque de ransomware. Para verificar la utilización, revise el valor de la columna Capacidad utilizada. Pase el cursor por encima de los valores para ver los porcentajes de espacio utilizado y libre. ○ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura. <p>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</p>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento & Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> • En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes. • En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios. • Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>10 Supervise los procesos de réplica de nodo.</p>	<ol style="list-style-type: none"> Para obtener el estado global de los procesos de réplica de nodo, vea el área Réplica en la página Centro de operaciones Descripción general. Para ver información sobre cada par de servidores replicados, pulse el área de réplica. Atención: Si observa un incremento inesperado en el número de anomalías de réplica, podría indicar un ataque de ransomware. Investigue la causa de las anomalías. Para ver la cantidad de datos que se ha duplicado durante las dos últimas semanas y la velocidad de la duplicación, seleccione un par de servidores y pulse Detalles. Para ver la información de réplica para un cliente, en la página Centro de operaciones Descripción general, pulse Clientes. Vea la información en la columna Carga de trabajo de réplica. Atención: Si observa un incremento drástico e inesperado en la carga de trabajo de réplica, podría indicar un ataque de ransomware. Investigue la causa del incremento en la carga de trabajo. 	<p>Para la supervisión avanzadas, vea la información sobre cómo ejecutar y finalizar procesos de réplica de nodos utilizando mandatos:</p> <ol style="list-style-type: none"> En la página Descripción general del Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. Emita el mandato QUERY REPLICATION. Para obtener instrucciones, consulte QUERY REPLICATION (Consultar los procesos de réplica de nodos). Si la operación de réplica se ha completado satisfactoriamente, el valor de Total de archivos a replicar coincide con el valor de Total de archivos replicados. <p>Para mostrar mensajes que están relacionados con el proceso de duplicación de un nodo en un servidor de réplica de origen o destino, complete los pasos siguientes:</p> <ol style="list-style-type: none"> En la página Visión general del Centro de operaciones pulse Servidores. Seleccione el servidor de réplica de origen o destino y pulse Detalles: <ul style="list-style-type: none"> Para ver tareas activas, pulse Tareas activas, seleccione la tarea y verifique que se muestra el estado En ejecución. Para obtener detalles, consulte los registros de actividad relacionados. Para ver las tareas completadas, pulse Tareas completadas, seleccione la tarea y asegúrese de que se visualiza el estado Completado. Para obtener detalles, consulte los registros de actividad relacionados.

Lista de comprobación de supervisión periódica

Para asegurarse de que la solución opera correctamente, complete las tareas en la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.










Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>. Busque el servidor asociado al cliente. 2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>. 3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>. 4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones que encontrará en QUERY ACTLOG (Consultar las anotaciones de actividades). 5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa. <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>. 2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>. 3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>. 	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento comunes del cliente</i>.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> 1. En la página <i>Centro de operaciones Descripción general</i>, pulse <i>Agrupaciones</i>. 2. Seleccione una agrupación y pulse <i>Vista rápida</i>. 3. En el área <i>Optimización de almacenamiento de datos</i>, vea la fila <i>Espacio guardado</i>. 	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores de nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la página <i>Descripción general de Centro de operaciones</i>, pase el ratón sobre el icono de configuración  y pulse <i>Creador de mandatos</i>. 2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones que encontrará en GENERATE DEDUPSTATS (Generar estadísticas de deduplicación de datos respecto a una agrupación de almacenamiento de contenedores de directorio). 3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones que encontrará en QUERY DEDUPSTATS (Consultar las estadísticas de deduplicación de datos).

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory query option devconfig</pre> 3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo. <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	




Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine si está disponible espacio suficiente para el sistema de archivos del directorio de la instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad. <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX •  Sistemas operativos Linux /home/tsminst1/tsminst1 •  Sistemas operativos Windows C:\tsminst1 <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Clientes. 2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente. 3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades. 4. En el área Última sesión, visualice la fila Enviado a cliente. 	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p> <p>Revise de forma periódica la tabla de resumen de actividad SQL, que contiene estadísticas sobre las sesiones de cliente. Para comparar la actividad actual con la actividad previa, utilice una sentencia SQL SELECT. Si el nivel de actividad es significativamente diferente de la actividad anterior, puede que indique un ataque de ransomware.</p> <p>Revise de forma periódica el registro de actividad. Busque los mensajes de ANE que indican a cuántos archivos se les realizó copia de seguridad y fueron inspeccionados. Compare los índices de deduplicación de los datos actuales con los índices anteriores. Si se realizó una copia de seguridad a un número de archivos más alto de lo habitual, o el índice de deduplicación cae de forma inesperada a 0, puede indicar un ataque de ransomware.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones. 2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles. 	<p>Sugerencias:</p> <ul style="list-style-type: none"> • Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. 3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>. • Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>. • Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> • Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes > Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones. 2. Seleccione una planificación y pulse Detalles. 3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila. 4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado. 5. Pulse Guardar.
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores > Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. 2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).

Referencia relacionada:

-  [QUERY ACTLOG \(Consultar las anotaciones de actividades\)](#)
-  [UPDATE STGPOOL \(Actualizar una agrupación de almacenamiento\)](#)
-  [QUERY EXTENTUPDATES \(Consultar extensiones de datos actualizadas\)](#)

Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

Licencia de PVU



El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.

Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia. Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
Modelo frontal	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
Modelo suplementario	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
Modelo de PVU	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.</p>

Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.

- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

Procedimiento


Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

Resultados

Los informes habilitados se envían según los valores especificados.

Referencia relacionada:

 UPDATE ADMIN (Actualizar un administrador)

Gestión de operaciones para una solución de disco multisitio

Utilice esta información para gestionar operaciones para una solución de disco multisitio con IBM Spectrum Protect que incluye un servidor y utiliza la eliminación de datos duplicados para varias ubicaciones.

- **Gestión del Centro de operaciones**
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.
- **Protección de aplicaciones, máquinas virtuales y sistemas**
El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.
- **Gestión del almacenamiento de datos**
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Gestión de la réplica**
Utilice la réplica para la recuperación de datos en el sitio de recuperación tras desastre y para mantener el mismo nivel de archivos en los servidores de origen y de destino. Puede gestionar réplicas en el nivel de nodo. También puede proteger datos en el nivel de agrupación de almacenamiento.
- **Protección del servidor**
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Implementación de un plan de recuperación tras desastre**
Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para

garantizar una alta disponibilidad del servidor.

- Recuperación de pérdida de datos o de paradas del sistema
Puede utilizar IBM Spectrum Protect para recuperar los datos que se han perdido al producirse un siniestro o una parada del sistema. Puede recuperar agrupaciones de almacenamiento de contenedores de directorio, datos de cliente y bases de datos.

Gestión del Centro de operaciones

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Reinicio del asistente de configuración inicial
Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.
- Cambio del servidor concentrador
Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.
- Restauración de la configuración a un estado de preconfiguración
Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Adición y eliminación de servidores spoke

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

Acerca de esta tarea

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke
Puede eliminar un servidor spoke del Centro de operaciones.

Adición de un servidor de radio

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

Antes de empezar

Las comunicaciones entre el servidor spoke y el servidor concentrador deben asegurarse utilizando el protocolo de Seguridad de la capa de transporte (TLS). Para asegurar las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

Procedimiento

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
 - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.

- Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente a 14 días, si configura el servidor como un servidor de radio.

Eliminación de un servidor spoke

Puede eliminar un servidor spoke del Centro de operaciones.

Acerca de esta tarea

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

Procedimiento

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre_grupo* representa el nombre del grupo supervisado y *nombre_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```


Consejo: Si se suprime una definición de servidor inmediatamente después de que se haya eliminado del grupo supervisado, la información de estado del servidor puede permanecer en el Centro de operaciones indefinidamente.

Para evitar este problema, espere a que pase el intervalo de recopilación de estados antes de suprimir la definición de servidor. El intervalo de recopilación de estados se muestra en la página Valores del Centro de operaciones.

Inicio y detención del servidor web

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.





Procedimiento

1. Detener el servidor web.
 -  Sistemas operativos AIX Desde el directorio */installation_dir/ui/utls*, donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

```
./stopserver.sh
```

-  Sistemas operativos Linux Emita el mandato siguiente:

```
service opscenter.rc stop
```

-  Sistemas operativos Windows En la ventana Servicios, detenga el servicio de IBM Spectrum Protect Operations Center.
2. Inicie el servidor web.
-  Sistemas operativos AIX Desde el directorio `/installation_dir/ui/utls`, donde `installation_dir` representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:
- ```
./startserver.sh
```
-  Sistemas operativos Linux Emita los mandatos siguientes:
- Inicie el servidor:
- ```
service opscenter.rc start
```
- Reinicie el servidor:
- ```
service opscenter.rc restart
```
- Determine si el servidor se está ejecutando:
- ```
service opscenter.rc status
```
-  Sistemas operativos Windows En la ventana Servicios, inicie el servicio IBM Spectrum Protect Operations Center.

Reinicio del asistente de configuración inicial

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

Antes de empezar

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:




- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.




Acerca de esta tarea

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

Procedimiento

1. Detenga el servidor web de Centro de operaciones.
2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde `installation_dir` representa el directorio en el que está instalado Centro de operaciones:
 -  Sistemas operativos AIX  Sistemas operativos Linux `dir_instalación/ui/Liberty/usr/servers/guiServer`
 -  Sistemas operativos Windows `dir_instalación\ui\Liberty\usr\servers\guiServer`

Por ejemplo:

 -  Sistemas operativos AIX  Sistemas operativos Linux `opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer`
 -  Sistemas operativos Windows `c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer`
3. En el directorio `guiServer`, elimine el archivo `serverConnection.properties`.
4. Inicie el servidor web Centro de operaciones.
5. Abra el Centro de operaciones.
6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

Cambio del servidor concentrador

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

Procedimiento

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

Tareas relacionadas:

Reinicio del asistente de configuración inicial

Restauración de la configuración a un estado de preconfiguración

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Procedimiento

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
 - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
 - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restablezca los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.

Tareas relacionadas:

Reinicio del asistente de configuración inicial

Inicio y detención del servidor web

Protección de aplicaciones, máquinas virtuales y sistemas

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Gestión de operaciones de cliente
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.
- Gestión de actualizaciones del cliente
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- Poner fuera de servicio un nodo cliente
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- Desactivación de datos para liberar espacio de almacenamiento
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Adición de clientes

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

Acerca de esta tarea

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones que encontrará en Selección del software de cliente y planificación de la instalación.
2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones que encontrará en Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones que encontrará en Instalación y configuración de clientes.

Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

Acerca de esta tarea

La práctica preferida es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente para poder configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración en la documentación de producto para asegurarse de que se puede producir las operaciones planificadas.

Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
----------	------------------------	------------------------------

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de archivado y copia de seguridad realiza la copia de seguridad y el archivado de archivos y directorios de los servidores de archivos y las estaciones de trabajo en el almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none"> • Requisitos del cliente de archivado y copia de seguridad • Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux • Instalación del cliente de archivado y copia de seguridad de Windows
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM software de base de datos DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se han completado sin concluir servidores IBM Domino.	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se han completado sin concluir servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de DB2 en el servidor IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de Informix en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection for SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales almacenadas en un servidor centralizado, crear políticas de copia de seguridad y restaurar máquinas virtuales o archivos individuales.</p> <p>De forma alternativa, utilice el cliente de archivado y copia de seguridad para hacer la copia de seguridad y restauración de una máquina virtual de VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> • Instalación de Data Protection for Microsoft Hyper-V • Instalación y actualización de Data Protection for VMware • Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

Acerca de esta tarea

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el período de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro de cliente, se asigna un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activas* activo.

Cuando un cliente realiza la copia de seguridad o el archivado de un archivo, el archivo se vincula a una clase de gestión del conjunto de políticas activas activo del dominio de políticas. Una *clase de gestión* es el conjunto de claves de reglas para gestionar los datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo local editable del sistema cliente y en un conjunto de opciones de cliente en el servidor. Las opciones del conjunto de opciones de cliente en el servidor pueden alterar temporalmente las opciones del archivo de opciones del cliente local o añadirse a dichas opciones.

Procedimiento

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

Visualización de políticas

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

Procedimiento

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
 - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
Consejo: Para ayudar a garantizar que pueda recuperar los datos después de un ataque de ransomware, aplique las siguientes directrices:
 - Asegúrese de que el valor de la columna de copias de seguridad tiene un valor mínimo de 2. El valor preferido es 3, 4 o más.
 - Asegúrese de que el valor en la columna Mantener copias de seguridad extra tiene un valor mínimo de 14 días. El valor preferido es 30 o más días.
 - Asegúrese de que el valor de la columna Mantener archivados tiene un valor mínimo de 30 días.

Si el software de IBM Spectrum Protect for Space Management está instalado en el cliente, asegúrese de que se ha realizado una copia de seguridad de los datos antes de realizar la migración. En el mandato DEFINE MGMTCLASS o UPDATE MGMTCLASS, especifique MIGREQUIRESBKUP=YES. A continuación, siga las directrices de la sugerencia.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
 - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
 - c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

Edición de políticas

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
Añadir una clase de gestión	<ol style="list-style-type: none"> a. En la tabla Conjuntos de políticas, pulse +Clase de gestión. b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión. c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada. d. Pulse Añadir.
Suprimir una clase de gestión	<p>En la columna Clase de gestión, pulse -.</p> <p>Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.</p>
Establecer una clase de gestión como clase de gestión predeterminada	<p>En la columna Predeterminada para la clase de gestión, pulse el botón de selección.</p> <p>Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.</p>
Modificar una clase de gestión	<p>Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.</p>

6. Pulse Guardar.

Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:
 - a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
 - b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.
 - c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menús Centro de operaciones. Pulse Planificaciones.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
Modificar una planificación	<ol style="list-style-type: none">a. En la vista Planificaciones, seleccione la planificación y pulse Detalles.b. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas.c. Modifique los valores de la planificación y pulse Guardar.
Crear una planificación	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
 - a. En la página Visión general del Centro de operaciones, pase el ratón por encima del icono de configuración  y pulse Creador de mandatos.
 - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

Tareas relacionadas:

-  Ajuste de la planificación para las operaciones diarias

Registro de clientes

Registrar un cliente para garantizar que el cliente pueda conectarse con el servidor y el servidor pueda proteger los datos de cliente.

Antes de empezar

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.
Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
 - a. En la barra de menús de Centro de operaciones, pulse Clientes.
 - b. En la tabla Clientes, pulse + Cliente.
 - c. Complete los pasos en el asistente Añadir cliente:
 - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
 - ii. En la ventana Configuración, copie los valores de opción TCPSERVERADDRESS, TCPPOINT, NODENAME y DEDUPLICATION.
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
 - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
 - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
 - v. Pulse Añadir cliente.

Referencia relacionada:

- Opción Tcpserveraddress
- Opción Tcpport
- Opción Nodename
- Opción Deduplication

Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:

- Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"> ■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux ■ Instalación del cliente de archivado y copia de seguridad de Windows <p>Consejo: También puede actualizar los clientes existentes utilizando el Centro de operaciones. Para obtener instrucciones, consulte Planificación de actualizaciones del cliente.</p>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> ■ Instalación de Data Protection for Oracle ■ Instalación de Data Protection for SQL Server en Windows Server Core
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> ■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) ■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) ■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> ■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux ■ Instalación y actualización de IBM Spectrum Protect Snapshot for VMware ■ Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> ■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux ■ Instalación del cliente de archivado y copia de seguridad de Windows
Si planea crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo de cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> ■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSEVERADDRESS, TCPSPORT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente

(Registro de clientes).

- Para los clientes que están instalados en un sistema operativo AIX, Linux o Mac OS X, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
- Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt.

De forma predeterminada, los archivos de opciones están en el directorio de instalación.

3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de clientes en el cliente. Siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones que encontrará en Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones que encontrará en Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:
 - a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
 - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

Qué hacer a continuación

Para cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones que encontrará en Modificación del ámbito de una copia de seguridad de cliente.

Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

Acerca de esta tarea

El método preferido es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Utilizando el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que las operaciones planificadas se pueden producir.

Si la empresa utiliza una herramienta de planificación de terceros como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Normalmente, las herramientas de planificación de terceros inician los programas cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

Procedimiento

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones para el sistema operativo que está instalado en el nodo cliente.

AIX y Oracle Solaris

- a. Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Pulse la pestaña Cliente web.
- c. En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.

- d. Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- e. Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- f. Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- g. Para permitir que el aceptador de cliente se inicie automáticamente después del reinicio de un sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```

Linux

- a. Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Pulse la pestaña Cliente web.
- c. En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- d. Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- e. Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- f. Inicie el aceptador de cliente iniciando sesión con el ID de usuario root y emitiendo el mandato siguiente:

```
service dsmcad start
```

- g. Para permitir que el aceptador de cliente pueda iniciarse automáticamente después del reinicio de un sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

MAC OS X

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- c. Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- d. Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- e. Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

Windows

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- b. Consulte la información en la página Asistente del planificador y pulse Siguiente.
- c. En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- d. En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- e. Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- f. Complete la configuración paso a paso a través del asistente.
- g. Actualice el archivo de opciones de cliente, `dsm.opt`, y configure la opción `passwordaccess` como `generate`.
- h. Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- i. Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El servicio de planificador se ha iniciado y detenido automáticamente mediante el servicio aceptador de cliente, según sea necesario.

Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

Antes de empezar

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores de opción en el archivo de opciones de cliente que ha obtenido durante ese proceso. Puede utilizar los valores para especificar puertos.

Acerca de esta tarea

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

Procedimiento

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción `tcpport` en el archivo de opciones de cliente. La opción `tcpport` del archivo de opciones de cliente debe coincidir con la opción `TCPPORT` en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción `httpport` en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción `webports` en el archivo de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción `tcpadminport` de cliente debe coincidir con el valor de la opción de servidor `TCPADMINPORT`. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.

Gestión de operaciones de cliente

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

Acerca de esta tarea

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- Evaluación de errores en registros de errores de cliente
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

- **Detención y reinicio del aceptador de cliente**
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- **Restablecimiento de contraseñas**
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- **Modificación del ámbito de una copia de seguridad de cliente**
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Evaluación de errores en registros de errores de cliente

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

Antes de empezar

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación *Instalación del servicio de gestión de cliente*. Para obtener instrucciones sobre cómo verificar la instalación, consulte *Verificación de que el servicio de gestión de clientes está instalado correctamente*.

Procedimiento

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
 1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
 2. Pulse Detalles.
 3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
 4. Revise los mensajes de registro recuperados.
Sugerencias:
 - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
 - Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.
- 5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.
Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

Detención y reinicio del aceptador de cliente

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

Acerca de esta tarea

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

Procedimiento

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
 - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```


- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Iniciar y Aceptar.

Referencia relacionada:

 Resolución de problemas de planificación del cliente

Restablecimiento de contraseñas

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

Procedimiento

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre_nodo* especifica el nodo cliente y *nueva_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificada, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:
 1. Para proporcionar acceso al administrador al servidor, ejecute el mandato `UNLOCK ADMIN`. Para obtener instrucciones, consulte `UNLOCK ADMIN` (Desbloquear un administrador).
 2. Configure una contraseña nueva utilizando el mandato `UPDATE ADMIN`:

```
update admin nombre_admin nueva_contraseña forcepwreset=yes
```

donde `admin` especifica el nombre del administrador y `nueva_contraseña` especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:
 1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
 2. Si necesita desbloquear un nodo cliente, utilice el mandato `UNLOCK NODE`. Para obtener instrucciones, consulte `UNLOCK NODE` (Desbloquear un nodo de cliente).
 3. Genere una nueva contraseña ejecutando el mandato `UPDATE NODE`:

```
update node nombre_nodo nueva_contraseña forcepwreset=yes
```

donde `nombre_nodo` especifica el nombre del nodo y `nueva_contraseña` especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

Modificación del ámbito de una copia de seguridad de cliente

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Acerca de esta tarea

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones que encontrará en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Para obtener información detallada al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción `dominio`. Siga las instrucciones que encontrará en Opción de cliente Domain.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

Gestión de actualizaciones del cliente

Cuando hay disponible un `fixpack` o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"> • Planificación de actualizaciones del cliente
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> • Actualización de Data Protection for SQL Server • Instalación de Data Protection for Oracle • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> • Instalación y actualización de Data Protection for VMware • Instalación de Data Protection for Microsoft Hyper-V

Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot

- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
 1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
 2. Pulse Más > Poner fuera de servicio.
- Para poner fuera de servicio un nodo cliente utilizando un mandato administrativo, complete los pasos siguientes:
 1. Determine si el nodo cliente se ha configurado para la réplica de nodo emitiendo el mandato QUERY NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, ejecute el siguiente mandato:

```
query node austin format=detailed
```

Revise el campo de salida de Estado de réplica.

2. Si el nodo cliente se ha configurado para la réplica, elimine el nodo cliente de la réplica emitiendo el mandato REMOVE REPLNODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
remove replnode austin
```

3. Realice una de las siguientes acciones:

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
 - Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
 - Un valor null especifica que el nodo no está fuera de servicio.
 - Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

Proceso proceso	Descripción proceso	Estado proceso
----- 3	----- DECOMMISSION NODE	----- Número de objetos de copia de seguridad desactivados para el nodo NODE1: 8 objetos desactivados.

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

Referencia relacionada:

- [DECOMMISSION NODE \(Poner fuera de servicio un nodo de cliente\)](#)
- [DECOMMISSION VM \(Poner fuera de servicio una máquina virtual\)](#)
- [QUERY NODE \(Consultar nodos\)](#)
- [REMOVE REPLNODE \(Eliminar un nodo de cliente de la réplica\)](#)

Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

Referencia relacionada:

[DEACTIVATE DATA](#) (Desactivar datos para un nodo de cliente)

Gestión del almacenamiento de datos

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Auditoría de un contenedor de la agrupación de almacenamiento
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.
- Gestión de la capacidad de inventario
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- Gestión del uso de la memoria y del procesador
Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.
- Ajuste de actividades planificadas
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

Referencia relacionada:

[Tipos de agrupación de almacenamiento](#)

Auditoría de un contenedor de la agrupación de almacenamiento

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.

Acerca de esta tarea

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

Procedimiento

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 000000000000076c.dcf:

```
audit container c:\tssm-storage\07\000000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

Qué hacer a continuación

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Puede reparar el contenido de la agrupación de almacenamiento utilizando el mandato REPAIR STGPOOL.

Restricción: Solo puede reparar el contenido de la agrupación de almacenamiento si ha protegido dicha agrupación de almacenamiento mediante el mandato PROTECT STGPOOL.

Referencia relacionada:

[AUDIT CONTAINER](#) (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

[QUERY DAMAGED](#) (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

Procedimiento

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
 - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
 - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.
Sugerencias:
 - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
 - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
 - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
 - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.
- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:
Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
```

```
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
 1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
 2. Detenga el servidor.
 3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
 5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

Referencia relacionada:

- ➔ ACTIVELOGSIZE, opción de servidor
- ➔ EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- ➔ SETOPT (Establecer una opción de servidor para actualización dinámica)

Gestión del uso de la memoria y del procesador

Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

Antes de empezar

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos admitidos para IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

Procedimiento

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.

2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

Procedimiento

1. Supervise el rendimiento del sistema de forma periódica para asegurarse de que las tareas de copia de seguridad de cliente y de mantenimiento de servidor se completan satisfactoriamente. Siga las instrucciones que encontrará en Supervisión de una solución de disco multisitio.
2. Opcional: Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, revise la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
 - o El número de clientes aumenta.
 - o La cantidad de datos de los que se hace copia de seguridad aumenta.
 - o La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución está funcionando en el nivel esperado. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
 - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
 - b. Pulse Detalles.
 - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos.


Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.

4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
 - a. Proteger agrupaciones de almacenamiento.
 - b. Replicar datos de nodo.
 - c. Realizar una copia de seguridad de la base de datos.
 - d. Ejecutar el proceso de caducidad para eliminar copias de seguridad de cliente y copias de archivo de archivado del almacenamiento de servidor.

Consejo: Planificar que las tareas de mantenimiento se inicien a una hora adecuada y en la secuencia correcta. Por ejemplo, planificar tareas de réplica después de que las copias de seguridad de cliente se completen satisfactoriamente.


- Traslado de clientes de un servidor a otro
Para evitar quedarse sin espacio en un servidor o para resolver problemas de carga de trabajo, es posible que tenga que mover los nodos cliente de un servidor a otro.

Conceptos relacionados:

 Rendimiento

Tareas relacionadas:

Definición de planificaciones para actividades de mantenimiento del servidor

 Deduplicación de datos (V7.1.1)

Gestión de la réplica

Utilice la réplica para la recuperación de datos en el sitio de recuperación tras desastre y para mantener el mismo nivel de archivos en los servidores de origen y de destino. Puede gestionar réplicas en el nivel de nodo. También puede proteger datos en el nivel de agrupación de almacenamiento.

- Compatibilidad de réplica
Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino son compatibles para la réplica.
- Habilitación de la réplica de nodo
Puede habilitar la réplica de nodo para proteger los datos.
- Protección de datos en agrupaciones de almacenamiento de contenedor de directorios
Proteja los datos de agrupaciones de almacenamiento de contenedor de directorios para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedor de directorios.

- Modificación de los valores de réplica
Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.
- Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino
Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

Compatibilidad de réplica

Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino son compatibles para la réplica.

Tabla 1. Compatibilidad de réplica de versiones de servidor

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V7.1	V7.1 o posterior
V7.1.1	V7.1 o posterior
V7.1.3	V7.1.3 o posterior
V7.1.4	V7.1.3 o posterior
V7.1.5	V7.1.3 o posterior
V7.1.6	V7.1.3 o posterior
V7.1.7	V7.1.3 o posterior
V7.1.8	V7.1.3 o posterior
V8.1	V7.1.3 o posterior
V8.1.1	V7.1.3 o posterior
V8.1.2	V7.1.3 o posterior
V8.1.3	V7.1.3 o posterior

Habilitación de la réplica de nodo

Puede habilitar la réplica de nodo para proteger los datos.

Antes de empezar

Asegúrese de que los servidores de origen y destino son compatibles para la réplica.

Acerca de esta tarea

Replique el nodo de cliente para replicar todos los datos de cliente, incluyendo metadatos. De forma predeterminada, la réplica de nodo está inhabilitada, cuando se inicia el servidor por primera vez.

Sugerencias:

- Para reducir el tiempo de proceso de réplica, proteja la agrupación de almacenamiento antes de replicar los nodos de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya se han replicado a través de la protección de agrupación de almacenamiento se omiten.
- La réplica requiere cantidades aumentadas de memoria y ancho de banda suficiente para completar el proceso. Cambie el tamaño de la base de datos y sus registros para garantizar que las transacciones se pueden completar.


Procedimiento

Para habilitar la réplica de nodo, complete los siguientes pasos en Centro de operaciones:

- En la página Servidores, pulse Detalles.
- En la página Detalles, pulse Propiedades.
- En la sección Réplica, seleccione Habilitada en el campo Réplica de salida.
- Pulse Guardar.

Qué hacer a continuación

Realice las acciones siguientes:

1. Para verificar que la réplica es correcta, revise Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor de IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología de Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos con el servidor remoto. Siga las instrucciones que encontrará en Determinación de si la tecnología de Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Referencia relacionada:

Compatibilidad de réplica

Protección de datos en agrupaciones de almacenamiento de contenedor de directorios

Proteja los datos de agrupaciones de almacenamiento de contenedor de directorios para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedor de directorios.

Antes de empezar

Asegúrese de que exista al menos una agrupación de contenedores en directorios en el servidor de réplica de destino. Cuando habilita la réplica en el Centro de operaciones, puede planificar la protección de agrupación de almacenamiento. Para configurar la réplica y habilitar la protección de agrupación de almacenamiento, complete los siguientes pasos:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
2. En la página de réplica, pulse Par de servidores.
3. Complete los pasos del asistente Añadir par de servidores.

Acerca de esta tarea

La protección de una agrupación de almacenamiento de contenedores de directorios hace copias de seguridad de extensiones en otra agrupación de almacenamiento y puede mejorar el rendimiento para la réplica de nodos. Cuando se inicia la réplica de nodo, se omiten las extensiones de datos de las que ya se han hecho copias de seguridad a través de la protección de la agrupación de almacenamiento, lo cual reduce el tiempo de proceso de la réplica. Puede planificar la protección de agrupaciones de almacenamiento varias veces al día para estar al día con los cambios realizados en los datos.

Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor. Debe utilizar agrupaciones de almacenamiento de contenedores de directorios si solo desea proteger y realizar la copia de seguridad de la agrupación de almacenamiento.

Estrategia de protección alternativa: Como alternativa al uso de la réplica, puede proteger los datos de las agrupaciones de almacenamiento de contenedores de directorios copiando los datos en agrupaciones de almacenamiento de copia de contenedor. Los datos de las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta. Las copias de cinta que se almacenan fuera del local proporcionan protección de recuperación tras desastre adicional en un entorno replicado.

Procedimiento

1. Como alternativa para habilitar la protección de agrupación de almacenamiento, puede utilizar el mandato PROTECT STGPOOL desde el servidor de origen para realizar la copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedor de directorios. Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio denominada POOL1, emita el siguiente mandato:

```
protect stgpool pool1
```

Como parte de la operación del mandato PROTECT STGPOOL, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato AUDIT CONTAINER podría identificar daños en la agrupación de almacenamiento de destino antes de que se emite el mandato PROTECT STGPOOL.

2. Opcional: Si las extensiones dañadas se han reparado en la agrupación de almacenamiento de destino y protege varias agrupaciones de almacenamiento de origen en una agrupación de almacenamiento de destino, complete los pasos siguientes para garantizar una reparación completa:
 - a. Emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen para reparar el máximo daño posible.

- b. Vuelva a emitir el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen. Para esta segunda operación, utilice el parámetro FORCERECONCILE=YES. Este paso garantiza que las reparaciones de otras agrupaciones de origen se reconocen correctamente para todas las agrupaciones de almacenamiento de origen.


Resultados

Si una agrupación de almacenamiento de contenedores de directorios está protegida, puede reparar la agrupación de almacenamiento si se producen daños, emitiendo el mandato REPAIR STGPOOL.




Restricción: Si duplica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorios, no puede reparar la agrupación de almacenamiento.

Qué hacer a continuación



Realice las acciones siguientes:

1. Para ver el estado de la carga de trabajo de la réplica, siga las instrucciones que encontrará en Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor de IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología de Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos con el servidor remoto. Siga las instrucciones que encontrará en Determinación de si la tecnología de Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Referencia relacionada:

-  Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedor de directorios
-  AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
-  PROTECT STGPOOL (Proteger datos de agrupación de almacenamiento)

Información relacionada:

-  Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de directorio
-  Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de nube

Modificación de los valores de réplica

Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.

Acerca de esta tarea

Es posible que tenga que personalizar los valores de réplica en los siguientes escenarios:

- Cambios en las prioridades de datos
- Cambios en reglas de réplica
- Requisito para que un servidor diferente sea el servidor de destino
- Procesos planificados que afectan de forma negativa al rendimiento de servidor

Procedimiento

Utilice Centro de operaciones para modificar valores de réplica.

Tarea	Procedimiento
Cambiar una regla de réplica.	<ol style="list-style-type: none">a. En la página Servidores, pulse Detalles.b. En la página Detalles, pulse Propiedades.c. En la sección Réplica, elija la regla de réplica que desea aplicar: Regla de archivado predeterminada, Regla de copia de seguridad predeterminada, o Regla de gestión de espacio predeterminada.d. Pulse Guardar.

Tarea	Procedimiento
Especifique el tiempo que se retienen los registros de réplica.	<ul style="list-style-type: none"> a. En la página Servidores, pulse Detalles. b. En la página Detalles, pulse Propiedades. c. En la sección Réplica, entre el número de días que deben retenerse los registros de réplica en el campo Retener historial de réplica. Sino, seleccione la casilla de verificación No retener si no necesita registros de réplica. d. Pulse Guardar.
Especifique un servidor de réplica de destino.	<ul style="list-style-type: none"> a. En la página Servidores, pulse Detalles. b. En la página Detalles, pulse Propiedades. c. En la sección Réplica, especifique el servidor de destino. d. Pulse Guardar.
Cancele un proceso de réplica.	<ul style="list-style-type: none"> a. En la página Servidores, pulse Tareas activas. b. Seleccione el proceso o sección que desea cancelar. c. Pulse Cancelar.

Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino

Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

Procedimiento

- Desde el servidor de réplica fuente, valide la configuración de réplica y verifique que el servidor de réplica de origen se puede comunicar con el servidor de réplica de destino emitiendo el mandato VALIDATE REPLICATION. Por ejemplo, valide la configuración utilizando el nombre de un nodo de cliente que se está duplicando:

```
validate replication node1 verifyconnection=yes
```

- Desde el servidor de réplica fuente, emita el mandato VALIDATE REPLPOLICY para revisar las diferencias entre las políticas en los servidores de réplica fuente y de destino. Por ejemplo, para mostrar las diferencias entre las políticas en el servidor de origen y el servidor de destino, CVT_SRV2, emita el mandato siguiente desde el servidor de origen:

```
validate replpolicy cvt_srv2
```

- Actualice las políticas en el servidor de destino, si es necesario.
Consejo: Puede utilizar Centro de operaciones para modificar las políticas en el servidor de destino. Siga las instrucciones que encontrará en Edición de políticas.
Por ejemplo, para mantener versiones inactivas de archivos durante un periodo de tiempo más corto en el servidor de destino que en el servidor de origen, reduzca el valor de Copias de seguridad en las clases de gestión que se aplican a datos de cliente replicados.
- Permita al servidor de réplica de destino utilizar sus políticas para gestionar los datos del nodo de cliente replicado emitiendo el mandato SET DISSIMILARPOLICIES en el servidor de origen. Por ejemplo, para habilitar las políticas en el servidor de réplica de destino, CVT_SRV2, emita el mandato siguiente en el servidor de origen:

```
set dissimilarpolicies cvt_srv2 on
```

La próxima vez que se ejecuta el proceso de réplica, se utilizan las políticas en el servidor de réplica de destino para gestionar los datos del nodo del cliente duplicado.

Consejo: Si configura la réplica utilizando el Centro de operaciones y las políticas en los servidores de réplica de origen y destino no coinciden, se utiliza la política especificada para el servidor de réplica de origen. Si ha habilitado las políticas en el servidor de réplica de destino utilizando el mandato SET DISSIMILARPOLICIES, se utiliza la política especificada para el servidor de réplica de destino. Si el servidor de réplica de destino no tiene la política que utiliza el nodo en servidor de réplica de origen, se utiliza la política STANDARD.

Referencia relacionada:

- [EXPORT POLICY](#) (Exportar información de política)
- [SET DISSIMILARPOLICIES](#) (Habilitar las políticas en el servidor de réplica de destino para gestionar daños replicados)

- ➡ VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)
- ➡ VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

Protección del servidor

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- **Conceptos sobre la seguridad**
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- **Gestión de administradores**
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.
- **Cambio de los requisitos de contraseña**
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- **Protección de IBM Spectrum Protect en el sistema**
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días. El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos de cliente	<ul style="list-style-type: none">• REGISTER NODE• UPDATE NODE
Administradores	<ul style="list-style-type: none">• REGISTER ADMIN• UPDATE ADMIN
Servidores	<ul style="list-style-type: none">• DEFINE SERVER• UPDATE SERVER

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:


- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de

administrador desde cualquier sistema.

- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

Tareas relacionadas:

 Protección de las comunicaciones

Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente: a. Registre el administrador y especifique Pa\$#\$twO como contraseña ejecutando el siguiente mandato: <code>register admin admin1 Pa\$#\$twO</code> b. Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <code>grant authority admin1 classes=system</code>
Cambie los permisos del administrador.	Cambie el nivel de autorización de un administrador, ADMIN1. • Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <code>grant authority admin1 classes=system</code> • Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <code>revoke authority admin1 classes=system</code>
Elimine administradores.	Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect: <code>remove admin admin1</code>
Impida el acceso al servidor de forma temporal.	Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.

Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, haga clic en el separador Propiedades.Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos. <p>El valor predeterminado en la instalación es 0.</p>
Establezca una longitud mínima para las contraseñas.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, pulse el separador Propiedades.Establezca el número de caracteres en el campo Longitud de contraseña mínima.
Establezca el periodo de caducidad para las contraseñas.	<ol style="list-style-type: none">En la página Servidores del Centro de operaciones, seleccione el servidor.Pulse Detalles y, a continuación, pulse el separador Propiedades.Establecer el número de días en el campo Caducidad común de la contraseña.
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.</p> <p>Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

Conceptos relacionados:

- 🔗 Autenticación de usuarios de IBM Spectrum Protect utilizando un servidor LDAP
- 🔗 Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

Protección de IBM Spectrum Protect en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.
- Limitación de acceso a través de restricciones de puerto
Limitar acceso al servidor aplicando restricciones de puerto.

Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
 - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
 - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grabe en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique el parámetro BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Limitación de acceso a través de restricciones de puerto

Limitar acceso al servidor aplicando restricciones de puerto.

Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPSPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPSPORT. Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPSPORT y SSLTCPSPORT.
SSLTCPSPORT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.

Opción de servidor	Acceso de puerto
SSLTCPADMINPORT	<p>Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.</p> <p>Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPOINT y SSLTCPPOINT.</p>

Restricciones:

Las restricciones siguientes se aplican cuando especifica los puertos de servidor solo SSL (SSLTCPPOINT y SSLTCPADMINPORT):

- Cuando especifique el puerto de servidor solo SSL para LLADDRESS en el mandato DEFINE SERVER o el mandato UPDATE SERVER, debe especificar también el parámetro SSL=YES.
- Cuando especifique el puerto de servidor solo SSL para la opción TCPPOINT del cliente, debe especificar también YES para la opción del cliente SSL.

Referencia relacionada:

Planificación del acceso de cortafuegos

Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- **Inicio del servidor para tareas de mantenimiento o reconfiguración**
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Detención del servidor

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

Acerca de esta tarea

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

Procedimiento

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:
 - a. En la página Visión general del Centro de operaciones, vea el área Actividad para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se

- visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.
- b. Vea el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:
 - El periodo actual, es decir, el periodo de 24 horas más reciente
 - El periodo anterior, es decir, 24 horas antes del periodo actualSi el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.
 - c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.
3. Espere hasta que las sesiones de nodo cliente se completen o cancelélas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:
- En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
 - Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
 - Pulse Cancelar.
 - Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.
- Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.
4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Inicio del servidor para tareas de mantenimiento o reconfiguración

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, dsmserv.opt, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

Procedimiento

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```




Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

Qué hacer a continuación

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
 - o  Sistemas operativos AIX Inicio de la instancia de servidor
 - o  Sistemas operativos Linux Inicio de la instancia de servidor
 - o  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

Planificación para actualizar el servidor

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

Acerca de esta tarea

Siga estas directrices:




- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

Procedimiento

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

Qué hacer a continuación

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

Preparación para una parada o actualización de sistema

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

Acerca de esta tarea

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor.

Procedimiento

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:

- a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
 - b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
 - c. Pulse Cancelar.
2. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

Implementación de un plan de recuperación tras desastre

Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

Acerca de esta tarea

Determine los requisitos que necesita para recuperación tras desastre identificando las prioridades empresariales respecto a la recuperación de nodo de cliente, los sistemas que utiliza para recuperar datos y si los nodos de cliente tienen conectividad con el servidor de recuperación. Utilice la réplica y la protección de agrupación de almacenamiento para proteger datos. También debe determinar la frecuencia con la que se protegen las agrupaciones de almacenamiento de contenedores de directorio.

- Realización de la obtención de detalles de recuperación
Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

Recuperación de pérdida de datos o de paradas del sistema

Puede utilizar IBM Spectrum Protect para recuperar los datos que se han perdido al producirse un siniestro o una parada del sistema. Puede recuperar agrupaciones de almacenamiento de contenedores de directorio, datos de cliente y bases de datos.

Antes de empezar

Planifique las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Emita los mandatos PROTECT STGPOOL y REPLICATE NODE como parte de la planificación. Proteja la agrupación de almacenamiento antes de replicar el nodo de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya están replicadas a través de la protección de agrupación de almacenamiento se omiten, lo que reduce el tiempo de proceso de réplica.

Procedimiento

Utilice los siguientes métodos de recuperación basándose en el componente que debe recuperar.

Componente a recuperar	Procedimiento	Más información
------------------------	---------------	-----------------

Componente a recuperar	Procedimiento	Más información
Agrupación de almacenamiento de contenedores de directorio	<p>Para recuperar agrupaciones de almacenamiento de contenedores de directorio, complete los siguientes pasos:</p> <ol style="list-style-type: none"> a. Explore las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio utilizando el mandato AUDIT CONTAINER y especificando el parámetro ACTION=SCANALL. b. Repare las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio utilizando el mandato REPAIR STGPOOL. Restricción: Solo puede reparar una agrupación de almacenamiento si dicha agrupación de almacenamiento está protegida. c. Elimine las extensiones de datos dañadas utilizando el mandato AUDIT CONTAINER y especificando el parámetro ACTION=REMOVEDAMAGED. 	Reparación de agrupaciones de almacenamiento

Componente a recuperar	Procedimiento	Más información
Datos de cliente	<p>Requisitos previos:</p> <ul style="list-style-type: none"> El servidor de réplica de origen, el servidor de réplica de destino y el cliente deben estar en el nivel V7.1 o posterior. Si alguno de los servidores está en un nivel anterior, la migración tras error automática se inhabilita y debe confiar en la migración tras error manual. <p>Configure manualmente el cliente para migrar tras error automáticamente al servidor de destino para la recuperación de datos.</p> <p>Si ha habilitado el cliente para una migración tras error de cliente automatizada, puede recuperar los datos utilizando la función de migración tras error automática. Puede verificar que la opción <code>usereplicationfailover</code> no está en el archivo de opciones de cliente o está establecida en <code>si</code>. Recupere datos del servidor de destino cuando el servidor de destino no esté disponible debido a una parada utilizando la migración tras error automática.</p> <p>Consejo:</p> <ul style="list-style-type: none"> Utilice el mandato <code>SET FAILOVERHLADDRESS</code> para especificar la dirección IP para el servidor de réplica durante la migración tras error, si la dirección es diferente de la dirección IP especificada para el proceso de réplica. 	<ul style="list-style-type: none"> Recuperación de datos dañados de una copia replicada <code>SET FAILOVERHLADDRESS</code> (Establecer una dirección de alto nivel de migración tras error)
Base de datos	<p>Requisitos previos:</p> <ul style="list-style-type: none"> Para restaurar la base de datos después de un siniestro, debe tener una copia del archivo de configuración del dispositivo actual. El archivo de configuración del dispositivo no se puede volver a crear. Asegúrese de que tiene una versión de seguridad de la base de datos. <p>Restaura la base de datos de IBM Spectrum Protect al estado más actual o a un punto específico en el tiempo utilizando el programa de utilidad del servidor <code>DSMSERV RESTORE DB</code>.</p>	<p><code>DSMSERV RESTORE DB</code> (Restaurar la base de datos)</p>


- Restauración de la base de datos


Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base

de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

- Recuperación de datos dañados de una copia replicada
Si no hay disponible un servidor de réplica de origen, puede recuperar los datos dañados de la copia replicada almacenada en el servidor de réplica de destino.
- Reparación de agrupaciones de almacenamiento
Si se ha producido un desastre o parada del sistema, puede reparar las extensiones de datos duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio.

Referencia relacionada:

 [AUDIT CONTAINER](#) (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

 [DSMSERV RESTORE DB](#) (Restaurar la base de datos)

Restauración de la base de datos

Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

Antes de empezar

Si los directorios de la base de datos y el registro de recuperación se han perdido, vuelva a crearlos antes de emitir el programa de utilidad del servidor DSMSERV RESTORE DB. Por ejemplo, utilice los mandatos siguientes:

 **Sistemas operativos Linux**

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

 **Sistemas operativos Windows**

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Restricciones:

- Para restaurar la base de datos a la versión más reciente, debe ubicar el directorio de registro de archivado. Si no puede ubicar el directorio, puede restaurar la base de datos sólo en un momento específico.
- No puede utilizar la capa de sockets seguros (SSL) para las operaciones de restauración de la base de datos.
- Si el nivel de release de la copia de seguridad de base de datos es diferente del nivel de release del servidor que se está restaurando, no puede restaurar la base de datos del servidor. Por ejemplo, si está utilizando un servidor de la Versión 8.1 e intenta restaurar una base de datos de la Versión 7.1, se produce un error.

Acerca de esta tarea

Las operaciones de restauración en un momento específico se utilizan generalmente para situaciones como la recuperación tras desastre o para eliminar los efectos de errores que pueden provocar incoherencias en la base de datos. Para recuperar la base de datos al instante en que se ha perdido la base de datos, recupérela a su estado actual.

Procedimiento

Utilice el programa de utilidad del servidor DSMSERV RESTORE DB para restaurar la base de datos. En función de la versión de la base de datos que desee restaurar, elija uno de los siguientes métodos:

- Restablezca una base de datos a su versión más reciente. Por ejemplo, utilice este mandato:

```
dsmserv restore db
```

- Restaure una base de datos a un momento específico. Por ejemplo, para restaurar la base de datos a una serie de copias de seguridad que se ha creado el 19 de abril de 2015, utilice el siguiente mandato:

```
dmserv restore db todate=04/19/2015
```

Qué hacer a continuación

Si ha restaurado la base de datos y existen agrupaciones de almacenamiento de contenedores de directorio en el servidor, debe identificar las incoherencias entre la base de datos y el sistema de archivos.

1. Si ha restaurado la base de datos a un punto en el tiempo y no ha retardado la reutilización de la agrupación de almacenamiento de contenedores de directorio, debe auditar todos los contenedores. Para auditar todos los contenedores, emita el siguiente mandato:

```
audit container stgpool
```

2. Si el servidor no puede identificar contenedores en el sistema, complete los pasos siguientes para mostrar una lista de contenedores:

- a. Desde un cliente administrativo, emita el mandato siguiente:


```
select container_name from containers
```

- b. Desde el sistema de archivos, emita el siguiente mandato para el directorio de la agrupación de almacenamiento en el servidor de origen:

Consejo: El directorio de la agrupación de almacenamiento se visualiza en la salida del mandato:

 Sistemas operativos AIX  Sistemas operativos Linux


```
[root@source]$ ls -lR
```

 Sistemas operativos Windows


```
c:\source_stgpooldir>dir /s
```


- c. Compare los contenedores listados en el sistema de archivos y el servidor.
- d. Emita el mandato AUDIT CONTAINER y especifique el contenedor que falta de la salida del servidor. Especifique el parámetro ACTION=REMOVEDAMAGED para suprimir el contenedor.
- e. Para asegurarse de que los contenedores se suprimen en el sistema de archivos, revise los mensajes que se muestran. Consejo: El servidor de IBM Spectrum Protect no reconoce los contenedores que se han creado desde la última copia de seguridad de la base de datos. Suprima los archivos adicionales que hay en su sistema de archivos local cuando compara con los archivos que existen en el servidor de IBM Spectrum Protect.

Tareas relacionadas:

 [Réplica de datos de nodo de cliente después de una restauración de la base de datos \(V7.1.1\)](#)

Referencia relacionada:

 [AUDIT CONTAINER \(Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio\)](#)

 [DSMSERV RESTORE DB \(Restaurar la base de datos\)](#)

Recuperación de datos dañados de una copia replicada

Si no hay disponible un servidor de réplica de origen, puede recuperar los datos dañados de la copia replicada almacenada en el servidor de réplica de destino.

Antes de empezar

El nombre del servidor que especifica con el mandato SET REPLSERVER debe coincidir con el nombre de una definición de servidor existente. También debe ser el nombre del servidor que se va a utilizar como servidor de réplica de destino. Si el nombre de servidor especificado por este mandato no coincide con el nombre de servidor de una definición de servidor existente, el mandato falla.

Consejo:

- Tenga cuidado cuando cambie o elimine un servidor de réplica de destino. Si cambia un servidor de réplica de destino, los datos de nodo cliente replicados se envían a un servidor de réplica de destino diferente. Si elimina un servidor de réplica de destino, los datos del nodo cliente no se replican.

Procedimiento

1. Verifique el estado de réplica de los datos en el servidor de destino. El estado indica si la réplica de copia de seguridad más reciente se ha replicado en el servidor secundario.
2. Restaure los datos desde un servidor de réplica de destino estableciendo el servidor de réplica de origen como servidor de réplica de destino. Por ejemplo, si desea establecer el servidor de réplica de origen como servidor de réplica de destino, server1, emita el siguiente mandato:

```
set replserver server1
```

Qué hacer a continuación

Al restaurar la base de datos de IBM Spectrum Protect en un servidor de réplica de origen, la réplica se inhabilita automáticamente. Antes de volver a habilitar la réplica, determine si las copias de datos que están en el servidor de réplica de destino son necesarias.

Tareas relacionadas:

➔ Réplica de datos de nodo de cliente después de una restauración de la base de datos (V7.1.1)

Reparación de agrupaciones de almacenamiento

Si se ha producido un desastre o parada del sistema, puede reparar las extensiones de datos duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio.

Antes de empezar

Identifique las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio utilizando el mandato AUDIT CONTAINER. Mediante la identificación de las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar.

Antes de reparar una agrupación de almacenamiento, asegúrese de que la agrupación de almacenamiento esté protegida mediante el mandato PROTECT STGPOOL.

Procedimiento

1. Para reparar una agrupación de almacenamiento de contenedores de directorio, utilice el mandato REPAIR STGPOOL. Por ejemplo, para reparar una agrupación de almacenamiento, STGPOOL1, emita el mandato siguiente:

```
repair stgpool stgpool1
```
2. Si la agrupación de almacenamiento dañada se especifica como una agrupación de almacenamiento de destino en el mandato PROTECT STGPOOL para una o varias agrupaciones de almacenamiento de origen, emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen.
3. Para asegurarse de que todos los datos dañados se identifiquen y reparen desde otras agrupaciones de almacenamiento de origen, emita el mandato PROTECT STGPOOL de nuevo desde todas las agrupaciones de almacenamiento de origen y especifique el parámetro FORCERECONCILE=YES.
4. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
5. Si la agrupación de almacenamiento dañada es una agrupación de almacenamiento de destino para la réplica de nodos de uno o varios servidores de origen, emita el mandato REPLICATE NODE de nuevo desde todos los servidores de origen.
6. Cuando el daño esté reparado, emita el mandato PROTECT STGPOOL para asegurarse de que la agrupación de almacenamiento esté protegida en otra agrupación de almacenamiento de contenedores de directorios.

Qué hacer a continuación

Asegúrese de que las extensiones de datos no dañadas se visualizan en la salida utilizando el mandato QUERY DAMAGED.

Referencia relacionada:

- ➔ Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedor de directorios
- ➔ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- ➔ QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)
- ➔ REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

Solución de cinta

Esta solución de protección de datos proporciona almacenamiento a soportes de cinta, una opción flexible y asequible para la retención de datos a largo plazo.

- Planificación de una solución de protección de datos basada en cinta
Planifique una solución de protección de datos que incluya operaciones de copia de seguridad de disco a cinta y de disco a disco a cinta para optimizar el almacenamiento.
- Implementación de una solución de protección de datos basada en cinta
Implemente la solución basada en cinta, que utiliza copia de seguridad 'de disco a disco a cinta' y disco intermedio para optimizar el almacenamiento. Al implementar la solución de cinta, puede habilitar la retención de datos a largo plazo y lograr una escalabilidad de bajo coste.
- Supervisión de una solución de cinta
Tras implementar una solución basada en cinta de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.
- Gestión de operaciones para una solución de cinta
Utilice esta información para gestionar las operaciones para una implementación de cinta para un servidor IBM Spectrum Protect.

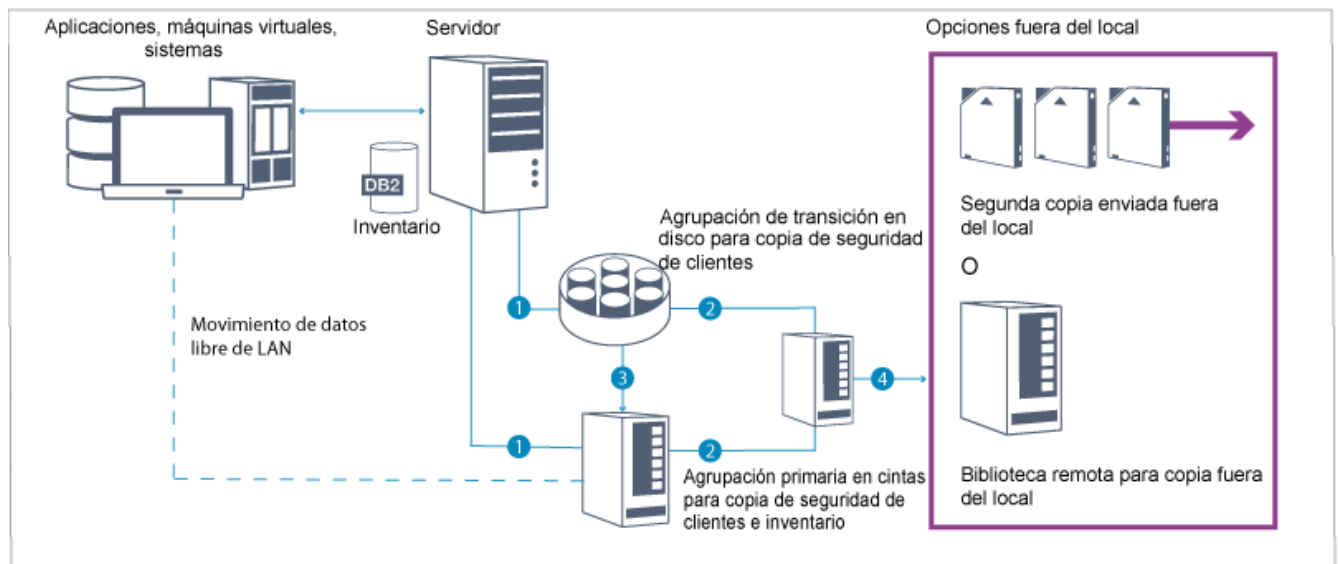
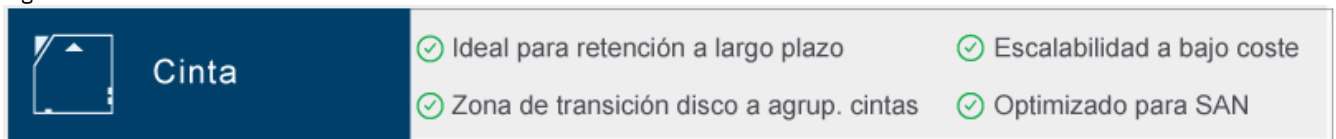
Planificación de una solución de protección de datos basada en cinta

Planifique una solución de protección de datos que incluya operaciones de copia de seguridad de disco a cinta y de disco a disco a cinta para optimizar el almacenamiento.

Hoja de vía de acceso de planificación

Planifique la solución de cinta revisando el diseño de la arquitectura en Figura 1 y completando después las tareas de la hoja de ruta que siguen al diagrama.

Figura 1. Solución de cinta



En esta configuración de protección de datos, el servidor utiliza hardware de almacenamiento de disco y de cinta. Se utiliza la transferencia de agrupaciones de almacenamiento, en la que los datos de cliente se almacenan inicialmente en agrupaciones de almacenamiento de disco y, a continuación, se migran a las agrupaciones de almacenamiento de cinta. Para la recuperación tras desastre, los volúmenes de cinta se pueden almacenar fuera del local. Las opciones fuera del local incluyen que un transportista mueva físicamente una segunda copia fuera del local o electrónicamente copias de cámara de seguridad fuera del local a una biblioteca remota.

Consejo: La solución descrita no incluye réplica de nodo. Sin embargo, si quiere utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento de disco a disco, asegúrese de que la operación de réplica esté completada antes de

migrar los datos de disco a disco. También puede utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento en un dispositivo de cinta local a una agrupación de almacenamiento de copia en un dispositivo de cinta local. Para planificar una solución basada en cinta, complete las tareas siguientes:

1. Ajustese a los requisitos de sistema para hardware y software.
2. Registre los valores de configuración del sistema en las hojas de trabajo de planificación.
3. Planifique el almacenamiento en disco.
4. Planifique el almacenamiento en cinta.
5. Planifique la seguridad.

Requisitos de planificación de cinta

Antes de implementar una solución de cinta, revise las directrices generales sobre los requisitos del sistema. Determine si realizar una copia de seguridad de los datos en un disco o en una cinta, o si combinar ambos sistemas.

Ancho de banda de red

La red debe tener suficiente ancho de banda para las transferencias de datos esperadas entre el cliente y el servidor, para la réplica y para las operaciones de restauración entre sitios que son necesarias para la recuperación tras desastre. Utilice una red de área de almacenamiento (SAN) para transferir datos entre el servidor, los dispositivos de disco y los dispositivos de cinta. Para obtener más información, consulte Requisitos de hardware.

Migración de datos

Migre todos los datos de disco a cinta a diario. Especifique una clase de dispositivo FILE para las agrupaciones de almacenamiento basadas en disco. Planifique la migración para controlar cuándo se produce el procesamiento. Para impedir la migración automática basada en el umbral de migración, especifique un valor de 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG cuando emita el mandato DEFINE STGPOOL. Debe mantener al menos el 20% de las unidades de cinta disponibles para operaciones de restauración. Para utilizar hasta el 80% de las unidades de cinta disponibles y mejorar el rendimiento, especifique el parámetro MIGPROCESS.

Considere la siguiente información en base al tipo de datos que se migran:

- Utilice una cinta para realizar una copia de seguridad de los datos de clientes que tienen objetos de gran tamaño, como bases de datos.
Consejo: Consulte con el fabricante de unidades y cintas cuál es el tamaño de la base de datos adecuada para grabar a cinta.
- Utilice un disco para realizar una copia de seguridad de los datos de clientes que tienen objetos más pequeños.
- Para realizar una copia de seguridad de los datos directamente en una cinta, utilice el movimiento de datos sin LAN. Para obtener más información, consulte Configuración del movimiento de datos sin LAN.
- No realice la copia de seguridad de máquinas virtuales a cintas. Utilice una agrupación de almacenamiento basada en disco individual que no migre a una agrupación de almacenamiento basada en cinta. Para obtener más información sobre soporte de máquina virtual, consulte nota técnica 1239546.

Capacidad de agrupación de almacenamiento

Mantenga suficiente capacidad de la agrupación de almacenamiento para permitir 2 días de copias de seguridad de cliente y un almacenamiento intermedio de 20%. Es posible que tenga que planificar copias de seguridad completas durante varios días para asegurarse de que tiene suficiente espacio de agrupación de almacenamiento.

unidades de cinta

Revise las especificaciones del fabricante y estime la capacidad de una unidad de cinta. Determine la cantidad de espacio necesaria para operaciones de copia de seguridad y migración. Reserve el 20% de unidades de cinta para operaciones de restauración.

Referencia relacionada:

 [MIGRATE STGPOOL \(Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente\)](#)

Requisitos del sistema para una solución basada en cinta

Se proporcionan los requisitos de hardware y software para una solución de almacenamiento basada en cintas que tiene una tasa de ingestión de datos de 14 TB por hora.

Revise la información para determinar los requisitos de hardware y software para su entorno de almacenamiento. Es posible que tenga que realizar ajustes basados en el tamaño de su sistema.

- Requisitos de hardware
Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

- Requisitos de software

La documentación para la solución basada en cinta de IBM Spectrum Protect incluye tareas de instalación y configuración para sistemas operativos IBM® AIX, Linux y Microsoft Windows. Debe cumplir los requisitos de software mínimos que se indican.




Requisitos de hardware

Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

Para obtener más información sobre la planificación de dispositivos de disco, consulte [Planificación del almacenamiento en disco](#).

Para obtener más información sobre la planificación de dispositivos de cinta, consulte [Planificación del almacenamiento en cinta](#).

La tabla siguiente incluye requisitos de hardware mínimos para el servidor y el almacenamiento. Si utiliza particiones locales (LPAR) o particiones de trabajo (WPAR), ajuste los requisitos de red para tener en cuenta los tamaños de las particiones. Las cifras de la tabla se basan en una tasa de ingestión de datos de 14 TB por hora.

Componente de hardware	Requisitos del sistema
Procesador de servidor	 Sistemas operativos AIX 8 núcleos de procesador, 3,42 GHz o más rápido. Por ejemplo, utilice un servidor basado en procesador POWER8.  Sistemas operativos Linux  Sistemas operativos Windows 16 núcleos de procesador, 2,0 GHz o más rápido. Por ejemplo, utilice un procesador Intel Xeon.
Memoria de servidor	64 GB de RAM.
Red	El siguiente dimensionamiento gestiona aproximadamente 14 TB de datos por hora: <ul style="list-style-type: none"> • 10 Gb de Ethernet (un mínimo de cuatro puertos) • 8 Gb de adaptador de canal de fibra (un mínimo de cuatro puertos) El número de puertos depende del porcentaje de ingestión de datos diario en agrupaciones de almacenamiento de disco en comparación con almacenamiento de cinta. Utilice adaptadores de canal de fibra distintos para los datos de cinta y de disco.

Componente de hardware	Requisitos del sistema
Almacenamiento	<p>Disco</p> <p>En función de la cantidad de datos que esté grabando en el disco, especifique el número de discos que necesita.</p> <p>Asegúrese de que el rendimiento de entrada/salida (E/S) secuencial de la red de área de almacenamiento (SAN) se corresponde con el rendimiento de E/S de la red de la fila anterior.</p> <p>Por ejemplo, si tiene que realizar la copia de seguridad de 10 TB de datos en un período de cuatro horas, el rendimiento es de aproximadamente 700 MB por segundo. En este caso, el servidor requiere una red frontal (vía de acceso de cliente a servidor) que admita un rendimiento mínimo de 700 MB por segundo. El SAN de fondo (la vía de acceso del servidor al dispositivo de almacenamiento) también debe admitir un rendimiento mínimo de 700 MB por segundo.</p> <p>Para calcular la velocidad de disco necesaria, utilice las siguientes fórmulas:</p> $\frac{\text{(cantidad total de ingestión de datos diaria - cantidad de ingestión de datos diaria directamente en cinta)} \div \text{(Número de horas para operaciones de copia de seguridad de cliente)}}{\text{Megabytes de ingestión de datos en disco por hora}} =$ $\frac{\text{(Megabytes de ingestión de datos en disco por hora)} \div \text{(3600 segundos por hora)}}{\text{Megabytes de ingestión de datos por segundo que debe soportar la tecnología de disco}} =$ <p>Cinta</p> <p>Seleccione la tecnología de cinta que mejor se ajuste a los requisitos empresariales. Por ejemplo, utilice las unidades de cinta IBM Linear Tape-Open (LTO) o IBM TS1150. Asegúrese de que dispone de suficientes puntos de montaje para las operaciones de copia de seguridad de cliente y para la migración. Para obtener más información sobre la planificación de almacenamiento en cinta, consulte Planificación del almacenamiento en cinta. Para obtener una lista de dispositivos de cinta soportados, consulte IBM® Support Portal for IBM Spectrum Protect.</p> <p>Consejo: Para optimizar el movimiento de datos, utilice el movimiento de datos sin LAN.</p>
Adaptadores de E/S de SAN	<p>Separe la entrada/salida de cinta y de disco. Para obtener más información sobre la selección de un adaptador, consulte la documentación para productos de hardware Brocade y para las soluciones de almacenamiento de IBM Storwize.</p> <p>Disco</p> <p>Utilice al menos dos adaptadores.</p> <p>Cinta</p> <p>Utilice al menos dos adaptadores.</p>

Estimación de requisitos de espacio para Centro de operaciones

Los requisitos de hardware para Centro de operaciones se incluyen en la tabla anterior, excepto para la base de datos y el espacio de registro de archivado (inventario) que utiliza Centro de operaciones para contener registros para clientes gestionados.

Si no piensa instalar el Centro de operaciones en el mismo sistema que el servidor IBM Spectrum Protect, puede calcular los requisitos de sistema por separado. Para calcular requisitos del sistema para Centro de operaciones, consulte la calculadora de requisitos del sistema en la nota técnica 1641684.

La gestión de Centro de operaciones en el servidor IBM Spectrum Protect es una carga de trabajo que requiere espacio adicional para operaciones de base de datos en el servidor spoke y el servidor concentrador. La cantidad de espacio en el servidor concentrador para el registro de archivado es mayor si el servidor concentrador está supervisando uno o más servidores spoke. Revise las siguientes directrices para calcular cuánto espacio necesita el servidor IBM Spectrum Protect.

Espacio de base de datos para el Centro de operaciones

El Centro de operaciones utiliza aproximadamente 4,4 GB de espacio de base de datos por cada 1000 clientes supervisados en un servidor. Este cálculo se aplica a servidores concentradores y servidores spoke dentro de una configuración.

Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1000 clientes. Esta configuración tiene un total de 5000 clientes en los cuatro servidores. Cada servidor spoke

necesita 4,4 GB de espacio de base de datos. Si los servidores spoke están en IBM Spectrum Protect versión 8.1.2 o posterior, el servidor concentrador necesita 8,8 GB de espacio de base de datos para supervisar solo a sus 2000 clientes:

$$(4,4 \text{ GB} \times 2) = 8,8 \text{ GB}$$

Espacio de base de datos para datos gestionados

Datos gestionados es la cantidad de datos protegidos, incluyendo la cantidad de datos para todas las versiones retenidas.

- Para tipos de clientes que realizan una copia de seguridad siempre incremental, se puede utilizar la siguiente fórmula para calcular el total de datos gestionados:

$$\text{Frontal} + (\text{frontal} \times \text{tasa de cambio} \times (\text{retención} - 1))$$

Por ejemplo, si realiza la copia de seguridad de 100 TB de datos frontales, usa un periodo de retención de 30 días y cuenta con una tasa de cambio del 5%, calcule el total de datos gestionados mediante las siguientes cifras:

$$100 \text{ TB} + (100 \text{ TB} \times 0,05 \times (30-1)) = 245 \text{ TB de total de datos gestionados}$$

- Para tipos de clientes que realizan una copia de seguridad completa a diario, se puede utilizar la siguiente fórmula para calcular el total de datos gestionados:

$$\text{Frontal} \times \text{retención} \times (1 + \text{tasa de cambio})$$

Por ejemplo, si realiza la copia de seguridad de 10 TB de datos frontales, usa un periodo de retención de 30 días y cuenta con una tasa de cambio del 3%, calcule el total de datos gestionados mediante las siguientes cifras:

$$10 \text{ TB} \times 30 \times (1 + .03) = 309 \text{ TB de total de datos gestionados}$$

Datos no estructurados, promedio de tamaño de objeto: 4 MB

Datos estructurados, promedio de tamaño de objeto: 128 MB

Datos no estructurados, número de objetos =

$$(245 \text{ TB} \times 1024 \times 1024) / 4 \text{ MB} = 64225280$$

Datos estructurados, número de objetos =

$$(309 \text{ TB} \times 1024 \times 1024) / 128 \text{ MB} = 2531328$$

Número total de objetos: 66756608

Coste de los datos gestionados (1 KB por objeto) =

$$(66756608 \text{ KB}) / (1024 \times 1024) = 63,66 \text{ GB}$$

Planifique un 20% de espacio adicional para que los sistemas de base de datos no estén al 100% de capacidad:

$$\text{Requisitos de almacenamiento físico del total de la base de datos} = (\text{espacio de datos gestionados} + \text{espacio del centro de operaciones}) \times (1,20)$$

Para este ejemplo, debe calcular el espacio utilizando las siguientes cifras:

$$(66,33 \text{ GB} + 8,4 \text{ GB}) \times 1,20 = 76,41 \text{ GB}$$

Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 18 GB de espacio de registro de archivado cada 24 horas, por servidor, para cada 1000 clientes supervisados en dicho servidor. Además, para cada 1000 clientes que se supervisan en servidores spoke, se utiliza espacio de registro de archivado adicional en el servidor concentrador. Para servidores spoke en versión V8.1.2 o posterior, esta cantidad añadida es de 1,2 GB de espacio de registro de archivado en el servidor concentrador por 1000 clientes supervisados cada 24 horas.

Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1000 clientes. Esta configuración tiene un total de 5000 clientes en los cuatro servidores. Puede calcular el espacio de registro de archivado para el servidor concentrador utilizando la fórmula siguiente:

$$((18 \text{ GB} \times 2) + (1,2 \text{ GB} \times 3)) = 39,6 \text{ GB de espacio de registro de archivado}$$

Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en los requisitos de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos para una configuración en la que se supervisan servidores spoke V8.1.2 o versiones posteriores:

- Servidor concentrador: en el rango 39,6 GB - 66 GB
- Cada servidor spoke: en el rango 18 GB - 30 GB

Asigne espacio de registro de archivado para que pueda dar soporte al Centro de operaciones sin que afecte a las operaciones de servidor.

Requisitos de software

La documentación para la solución basada en cinta de IBM Spectrum Protect incluye tareas de instalación y configuración para sistemas operativos IBM® AIX, Linux y Microsoft Windows. Debe cumplir los requisitos de software mínimos que se indican.

Para obtener información sobre los requisitos de software para los controladores de dispositivo lin_tape de IBM, consulte IBM Tape Device Drivers Installation and User's Guide.

Sistemas AIX

Tipo de software	Requisitos mínimos de software
Sistema operativo	IBM AIX 7.1 Para obtener más información sobre los requisitos del sistema operativo, consulte AIX: requisitos mínimos del sistema para sistemas AIX.
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema antes de instalar o actualizar el servidor de IBM Spectrum Protect . Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.
Tipo de sistema de archivos	Sistemas de archivos JFS2 Los sistemas AIX pueden almacenar en caché una gran cantidad de datos del sistema de archivos y esto puede reducir la memoria que se necesita para el servidor y los procesos de IBM DB2. Para evitar la paginación con el servidor de AIX, utilice la opción de montaje rbrw mount para el sistema de archivos JFS2. Se utiliza menos memoria para la memoria caché de sistema de archivo y hay más disponible para IBM Spectrum Protect. No utilice las opciones de montaje del sistema de archivos, E/S simultáneas (CIO) y E/S directas (DIO), para sistemas de archivos que contengan la base de datos de IBM Spectrum Protect, registros o volúmenes de agrupaciones de almacenamiento. Estas opciones pueden producir la degradación del rendimiento de muchas operaciones de servidor. IBM Spectrum Protect y DB2 aún pueden utilizar DIO donde sea beneficioso hacerlo, pero IBM Spectrum Protect no necesita las opciones de montaje para aprovechar estas técnicas de forma selectiva.
Otro software	Shell Korn (ksh)

Sistemas Linux

Tipo de software	Requisitos mínimos de software
Sistema operativo	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	Bibliotecas de GNU C, versión 2.3.3-98.38 o posterior que está instalado en el sistema de IBM Spectrum Protect. Red Hat Enterprise Linux Servers: <ul style="list-style-type: none"> • libaio • libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits) • numactl.x86_64
Tipo de sistema de archivos	Formato de sistemas de archivos relacionados con bases de datos con ext3 o ext4. Para los sistemas de archivos relacionados con agrupaciones de almacenamiento, utilice XFS.
Otro software	Shell Korn (ksh)

Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS
Otro software	Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado. Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: <ul style="list-style-type: none"> Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador

Planificación de hojas de trabajo

Utilice las hojas de trabajo de planificación para registrar los valores que se utilizan para configurar el sistema y configurar el servidor de IBM Spectrum Protect. Utilice los valores predeterminados de prácticas recomendadas que aparecen en las hojas de trabajo.

Cada hoja de trabajo le ayuda a prepararse para diferentes partes de la configuración del sistema utilizando valores de las prácticas recomendadas:







Configuración previa de sistema servidor

Utilice las hojas de trabajo de configuración previa para planificar los sistemas de archivos y directorios que se crean al configurar sistemas de archivos para IBM Spectrum Protect durante la configuración del sistema. Todos los directorios que crea para el servidor deben estar vacíos.

Configuración del servidor

Utilice las hojas de trabajo de configuración cuando configure el servidor. Los valores predeterminados se recomiendan para la mayoría de los elementos, excepto donde se indica.

Tabla 1. Hoja de trabajo para la configuración previa de un sistema servidor

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Más información
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable.	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo. El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	 Sistemas operativos AIX  Sistemas operativos Linux /home/tsminst1/tsminst1  Sistemas operativos Windows C:\tsminst1		 Sistemas operativos AIX 50 GB.  Sistemas operativos Linux  Sistemas operativos Windows 25 GB.	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 2.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Más información
Directorio para la instalación del servidor	<ul style="list-style-type: none"> Sistemas operativos AIX Sistemas operativos Linux/ Sistemas operativos Windows C:		Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB. Sistemas operativos Linux Sistemas operativos Windows Espacio mínimo requerido para el directorio: 30 GB.	
Directorio para la instalación del servidor	/usr		Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	Sistemas operativos AIX/var		Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	Sistemas operativos AIX/tmp		Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	Sistemas operativos AIX/opt		Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 10 GB.	
Directorio para el registro activo	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMalog Sistemas operativos Windows C:\tsminst1\TSMalog		128 GB.	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.
Directorio para el registro de archivado	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMarchlog Sistemas operativos Windows C:\tsminst1\TSMarchlog		3 TB.	
Directorios para la base de datos	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 Sistemas operativos Windows C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03		Para obtener instrucciones sobre cómo calcular los requisitos de espacio, consulte Requisitos de hardware.	Cree cuatro sistemas de archivos para la base de datos.















Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Más información
Directorios para almacenamiento	 Sistemas operativos AIX  Sistemas operativos Linux /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...  Sistemas operativos Windows C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Determine la capacidad total mínima para todos los directorios utilizando el siguiente cálculo: Diariamente porcentaje de datos ingeridos que se graban en el disco + 20% = capacidad mínima total	El método preferido consiste en definir al menos un directorio para cada dispositivo de cinta.







Tabla 2. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Más información
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 1 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	 Sistemas operativos AIX  Sistemas operativos Linux passw0rd  Sistemas operativos Windows pAssW0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	 Sistemas operativos AIX  Sistemas operativos Linux tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.

Elemento	Valor predeterminado	Valor	Más información
Hora de inicio de la planificación	23:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p> <p>En esta guía, la hora sugerida de inicio de operaciones de copia de seguridad de cliente es 23:00.</p>

Tabla 3. Hoja de trabajo para la configuración de cinta

Elemento	Valor predeterminado	Valor	Más información
Archivos de dispositivos de robótica	<p>Dispositivos de IBM® con un controlador de dispositivo de cinta de IBM:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX /dev/smcX •  Sistemas operativos Linux /dev/IBMchangerX •  Sistemas operativos Windows ChangerX <p>Dispositivos no IBM con un controlador de dispositivo IBM Spectrum Protect</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX /dev/lbX •  Sistemas operativos Linux /dev/tsm SCSI/lbX •  Sistemas operativos Windows lbA.B.C.D 		<p>Para definir manualmente los archivos de dispositivo de biblioteca, utilice los siguientes mandatos:</p> <ul style="list-style-type: none"> • DEFINE LIBRARY • DEFINE DRIVE • DEFINE PATH <p>Para SCSI, puede utilizar el mandato PERFORM LIBACTION para definir todas las unidades y sus vías de acceso para una única biblioteca en un paso. Para utilizar este mandato para definir todas las unidades y vías de acceso, la opción SANDISCOVERY debe estar admitida y habilitada.</p>

Elemento	Valor predeterminado	Valor	Más información
unidades de cinta	<p>Dispositivos de IBM con un controlador de dispositivo de cinta de IBM:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX /dev/rmtX •  Sistemas operativos Linux /dev/IBMtapeX •  Sistemas operativos Windows TapeX <p>Dispositivos no IBM con un controlador de dispositivo IBM Spectrum Protect</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX /dev/mtX •  Sistemas operativos Linux /dev/tmscsi/mtX •  Sistemas operativos Windows mtA.B.C.D 		

Planificación del almacenamiento en disco

Elegir la tecnología de almacenamiento más efectiva para componentes de IBM Spectrum Protect para asegurarse de que el rendimiento de servidor y las operaciones son eficientes.

Los dispositivos de hardware de almacenamiento tiene características de rendimiento y capacidad diferentes, lo que determina cómo se pueden utilizar de forma eficaz con IBM Spectrum Protect. Para obtener una orientación general sobre cómo seleccionar el hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

Base de datos, registro activo y registro de archivado

- Utilice un disco de estado sólido (SSD) o un disco rápido de 15.000 rpm para el registro activo y la base de datos de IBM Spectrum Protect.
- Al crear matrices para la base de datos, utilice RAID nivel 5.
- Utilice discos separados para el almacenamiento de copia de seguridad de la base de datos y el registro de archivado.

Agrupación de almacenamiento

Utilice el nivel RAID 6 para las matrices de agrupación de almacenamiento para añadir protección frente a las anomalías de unidad doble cuando se utilizan tipos de disco de gran tamaño.

- Planificación de matrices de almacenamiento
Prepararse para la configuración de almacenamiento de disco planificando matrices RAID y volúmenes, de acuerdo con el tamaño del sistema IBM Spectrum Protect.

Planificación del almacenamiento en cinta

Determine qué dispositivos de cinta utilizar y cómo configurarlos. Para optimizar el rendimiento del sistema, planifique utilizar dispositivos de cinta rápidos y de gran capacidad. Suministre suficientes unidades de cinta para cumplir los requisitos empresariales.

- Dispositivos de cinta y bibliotecas soportados
El servidor puede utilizar una amplia variedad de dispositivos de cinta y bibliotecas. Seleccione dispositivos de cinta y bibliotecas que cumplan sus requisitos de negocio.
- Configuraciones de dispositivos de cinta soportadas
Revise la información sobre las redes de área local (LAN) y las redes de área de almacenamiento (SAN). Para optimizar el movimiento de datos, planifique la configuración del movimiento de datos sin LAN. Además, considere si utilizar el uso compartido de bibliotecas.
- Definiciones necesarias para dispositivos de almacenamiento en cinta
Para que el servidor de IBM Spectrum Protect pueda utilizar un dispositivo de cinta, debe configurar el dispositivo en el sistema




operativo y en el servidor. Durante el proceso de planificación, determine qué definiciones se necesitan para sus dispositivos de almacenamiento en cinta.

- Planificación de la jerarquía de agrupaciones de almacenamiento
Planifique la jerarquía de agrupaciones de almacenamiento para asegurarse de que los datos se migran a diario de disco a cinta. La migración libera espacio en el dispositivo de disco y mueve los datos a la cinta para la retención a largo plazo. De esta manera, podrá aprovechar la escalabilidad, la rentabilidad y las características de seguridad del almacenamiento de cintas.
- Almacenamiento de datos fuera del local
Para facilitar la recuperación de datos y como parte de la estrategia de recuperación tras desastre, almacene copias de cinta fuera del local.

Dispositivos de cinta y bibliotecas soportados

El servidor puede utilizar una amplia variedad de dispositivos de cinta y bibliotecas. Seleccione dispositivos de cinta y bibliotecas que cumplan sus requisitos de negocio.

Para obtener una lista de dispositivos soportados y formatos de clase de dispositivo válidos, consulte el sitio web de su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos soportados para AIX y Windows
-  Sistemas operativos Linux Dispositivos soportados para Linux

Para obtener más información acerca de los dispositivos y objetos de almacenamiento, consulte Tipos de dispositivos de almacenamiento.

Cada uno de los dispositivos definidos para IBM Spectrum Protect está asociado a una *clase de dispositivo*. Dicha clase de dispositivo especifica un tipo de dispositivo e información de gestión de medios, como por ejemplo el formato de grabación, la capacidad estimada y los prefijos de etiquetas.

El *tipo de dispositivo* identifica a un dispositivo como miembro de un grupo que comparte características de medios semejantes. Por ejemplo, el tipo de dispositivo LTO se aplica a todas las generaciones de unidades de cinta LTO.

Una clase de dispositivo para una unidad de cinta también debe especificar una biblioteca. Una *biblioteca física* es un conjunto de una o varias unidades que comparten requisitos semejantes de montaje de medios. Es decir, la unidad la puede montar un operador o un mecanismo de montaje automatizado.

Una *definición de objeto de biblioteca* especifica el tipo de biblioteca y otras características asociadas con el tipo de biblioteca.

La tabla siguiente muestra los tipos de biblioteca preferidos para una solución de cinta IBM Spectrum Protect versión 8.1.3.

Tabla 1. Tipos de biblioteca para una solución de cinta IBM Spectrum Protect 8.1.3

Tipo de biblioteca	Descripción	Más información
SCSI	Una biblioteca SCSI se controla mediante una interfaz SCSI, conectada directamente al host del servidor a través de cables SCSI o mediante una red de área de almacenamiento. Un robot u otro mecanismo maneja automáticamente el montaje y el desmontaje de los volúmenes de cinta. Si crea distintos tipos de unidades para una biblioteca SCSI, crea múltiples bibliotecas lógicas que no se pueden dividir entre distintos tipos de unidades. Una biblioteca SCSI puede contener unidades de tecnologías mixtas, incluyendo unidades LTO Ultrium y unidades DLT (Digital Linear Tape). Por ejemplo: <ul style="list-style-type: none"> • La biblioteca Oracle StorageTek L700 • El dispositivo de cinta IBM® 3592 	Configuración de bibliotecas para su uso por parte de un servidor Las restricciones se aplican cuando combina distintas generaciones de medios y unidades. Para obtener más información, consulte: <ul style="list-style-type: none"> • Combinación de generaciones de unidades y medios 3592 en una sola biblioteca • Combinación de unidades y medios LTO en una biblioteca
Compartidas	Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI. La biblioteca se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas. Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas. Las bibliotecas compartidas hacen referencia a un gestor de bibliotecas.	

Configuraciones de dispositivos de cinta soportadas

Revise la información sobre las redes de área local (LAN) y las redes de área de almacenamiento (SAN). Para optimizar el movimiento de datos, planifique la configuración del movimiento de datos sin LAN. Además, considere si utilizar el uso compartido de bibliotecas.

Seleccione la configuración de dispositivo que se ajuste a sus requisitos empresariales.

- **Movimiento de datos sin LAN y basados en LAN**
Puede mover datos entre clientes y dispositivos de almacenamiento que estén conectados a una red de área local (LAN), o a dispositivos de almacenamiento conectados a una red de área de almacenamiento (SAN), conocido como movimiento de datos sin LAN.
- **Compartición de bibliotecas**
Puede optimizar la eficiencia de su solución de cinta configurando la compartición de biblioteca. La compartición de biblioteca permite que diversos servidores de IBM Spectrum Protect utilicen la misma biblioteca de cintas y las mismas unidades en una red de área de almacenamiento (SAN) y permite mejorar el rendimiento de los procesos de copia de seguridad y recuperación y la utilización del hardware de cintas.
- **Movimiento de datos sin LAN**
IBM Spectrum Protect proporciona la capacidad para un cliente, a través de un agente de almacenamiento, de hacer copia de seguridad y restaurar datos directamente a una biblioteca de cintas en una SAN. Este tipo de movimiento de datos también se conoce como movimiento de datos sin LAN.
- **Mezcla de tipos de dispositivos en una biblioteca**
IBM Spectrum Protect admite mezclar diferentes tipos de dispositivos en una sola biblioteca automatizada, si la biblioteca puede distinguir entre los diferentes medios para los diferentes tipos de dispositivos. Para simplificar el proceso de configuración, no planifique mezclar distintos tipos de dispositivos en una misma biblioteca. Si tiene que combinar tipos de dispositivos, revise las restricciones.

Movimiento de datos sin LAN y basados en LAN

Puede mover datos entre clientes y dispositivos de almacenamiento que estén conectados a una red de área local (LAN), o a dispositivos de almacenamiento conectados a una red de área de almacenamiento (SAN), conocido como movimiento de datos sin LAN.

En una configuración de LAN convencional, hay una o más bibliotecas de cintas asociadas con un único servidor IBM Spectrum Protect. El movimiento de datos sin LAN pone el ancho de banda disponible para otros usos y disminuye la carga en el servidor IBM Spectrum Protect.

En una configuración de LAN, los datos de cliente, el correo electrónico, la conexión de terminal, el programa de aplicación y la información de control de dispositivo deben gestionarse a través de la misma red. La información sobre el control de dispositivos, las copias de seguridad de cliente y la restauración de datos se transfieren a través de la LAN.

Una red de área de almacenamiento (SAN) es una red de almacenamiento dedicada que puede mejorar el rendimiento del sistema.

Utilizando IBM Spectrum Protect en una SAN, puede beneficiarse de las siguientes funciones:

- **Compartir dispositivos de almacenamiento entre varios servidores de IBM Spectrum Protect.**
Restricción: Un dispositivo de almacenamiento con tipo de dispositivo GENERICTAPE no se puede compartir entre servidores.
- **Mover los datos de cliente de IBM Spectrum Protect directamente a los dispositivos de almacenamiento (movimiento de datos sin LAN) configurando un agente de almacenamiento en el sistema cliente.**

En una SAN, puede compartir unidades de cinta y bibliotecas soportadas por el servidor de IBM Spectrum Protect, incluyendo la mayoría de dispositivos de cinta SCSI.

Cuando los servidores IBM Spectrum Protect comparten una cinta SCSI, un servidor, el *gestor de biblioteca*, posee y controla el dispositivo. Los agentes de almacenamiento, junto con otros servidores de IBM Spectrum Protect que comparten esta biblioteca, son los *agentes de biblioteca*. Un cliente de biblioteca solicita recursos de biblioteca compartida como, por ejemplo, unidades o medios, al gestor de bibliotecas, pero utiliza los recursos de forma independiente. El gestor de bibliotecas coordina el acceso a estos recursos. Los servidores de IBM Spectrum Protect que se define como clientes de biblioteca utilizan comunicaciones de servidor a servidor para ponerse en contacto con el gestor de bibliotecas y solicitar el servicio de dispositivos. Los datos se traspasan por la SAN entre los servidores y el dispositivo de almacenamiento.

Requisito: Si define un servidor de gestor de biblioteca que se comparte con el servidor IBM Spectrum Protect, la opción SANDISCOVERY se debe establecer en ENCENDIDO. De forma predeterminada, esta opción está establecida en OFF.

Los servidores de IBM Spectrum Protect utilizan las características siguientes cuando comparten una biblioteca automatizada:

Particionamiento del inventario de volúmenes

El inventario de volúmenes de medios de la biblioteca compartida está particionado entre los servidores. O bien un servidor es propietario de un volumen determinado, o el volumen se encuentra en la agrupación de reutilización global. Ningún servidor es propietario de la agrupación de reutilizables.

Acceso a unidad serializado

Sólo un servidor accede a una unidad de cintas cada vez. El acceso a unidades está serializado. IBM Spectrum Protect controla el acceso a unidades para que los servidores no desmonten los volúmenes de otros servidores ni graben en unidades donde otros servidores montan sus volúmenes.

Acceso a montaje serializado

El cambiador automático de la biblioteca efectúa una única operación de montaje o desmontaje cada vez. El gestor de biblioteca completa todas las operaciones de montaje para proporcionar esta serialización.

Compartición de bibliotecas

Puede optimizar la eficiencia de su solución de cinta configurando la compartición de biblioteca. La compartición de biblioteca permite que diversos servidores de IBM Spectrum Protect utilicen la misma biblioteca de cintas y las mismas unidades en una red de área de almacenamiento (SAN) y permite mejorar el rendimiento de los procesos de copia de seguridad y recuperación y la utilización del hardware de cintas.

Cuando los servidores de IBM Spectrum Protect comparten una biblioteca, un servidor se configura como el gestor de bibliotecas y controla las operaciones de la biblioteca como, por ejemplo, el montaje y desmontaje. El gestor de bibliotecas también controla la propiedad del volumen y el inventario de la biblioteca. Otros servidores están configurados como clientes de biblioteca y utilizan las comunicaciones de servidor a servidor para ponerse en contacto con el gestor de bibliotecas y solicitar recursos.

Los clientes de biblioteca debe estar de la misma versión o de una versión anterior que el servidor del gestor de biblioteca. Un gestor de biblioteca no puede admitir clientes de biblioteca de una versión posterior. Para obtener más información, consulte Compatibilidad del agente de almacenamiento y el cliente de biblioteca con un servidor de IBM Spectrum Protect.

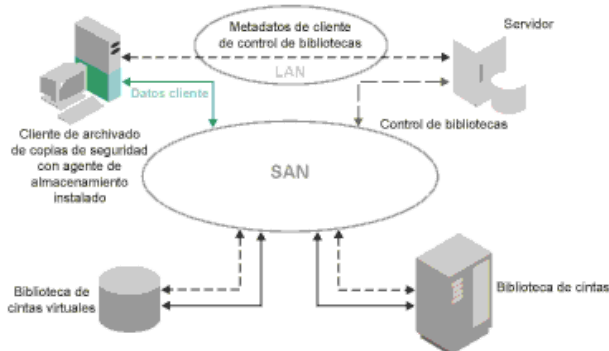
Movimiento de datos sin LAN

IBM Spectrum Protect proporciona la capacidad para un cliente, a través de un agente de almacenamiento, de hacer copia de seguridad y restaurar datos directamente a una biblioteca de cintas en una SAN. Este tipo de movimiento de datos también se conoce como movimiento de datos sin LAN.

Restricción: Los dispositivos de almacenamiento Centera no pueden ser destinos para las operaciones fuera de la LAN.

La Figura 1 muestra una configuración de SAN en la que un cliente accede directamente a una cinta para leer o grabar datos.

Figura 1. Movimiento de datos sin LAN



El movimiento de datos sin LAN requiere la instalación de un agente de almacenamiento en el sistema cliente. El servidor mantiene la base de datos, las anotaciones de recuperación y el gestor de biblioteca para controlar las operaciones de los dispositivos. El agente de almacenamiento del cliente gestiona la transferencia de datos al dispositivo de la SAN. Esta implementación libera ancho de banda de la LAN que, de otro modo, se utilizaría para la transferencia de datos del cliente.

Mezcla de tipos de dispositivos en una biblioteca

IBM Spectrum Protect admite mezclar diferentes tipos de dispositivos en una sola biblioteca automatizada, si la biblioteca puede distinguir entre los diferentes medios para los diferentes tipos de dispositivos. Para simplificar el proceso de configuración, no planifique mezclar distintos tipos de dispositivos en una misma biblioteca. Si tiene que combinar tipos de dispositivos, revise las restricciones.

Las bibliotecas con esta capacidad son los modelos que tienen unidades incorporadas mixtas, o que admiten la adición de unidades mixtas. Para obtener información sobre modelos específicos, consulte la documentación del fabricante. Para obtener más información acerca de las bibliotecas probadas en IBM Spectrum Protect con mezcla de tipos de dispositivos, consulte la información para su sistema operativo:

- Dispositivos de IBM Spectrum Protect admitidos AIX, HP-UX, Solaris y Windows
- Dispositivos de IBM Spectrum Protect admitidos para Linux

Por ejemplo, puede tener unidades LTO Ultrium y unidades TS4500 de IBM en una biblioteca única definida en el servidor de IBM Spectrum Protect.

- Diferentes generaciones de medios en una biblioteca
El servidor de IBM Spectrum Protect permite mezclar tipos de dispositivo en una biblioteca automatizada, pero normalmente no se admite mezclar distintas generaciones del mismo tipo de unidad. Las nuevas unidades no pueden grabar en los formatos de medios más antiguos y las unidades antiguas no pueden leer los formatos nuevos. Las unidades LTO Ultrium no son una excepción a esta regla.
- Mezcla de medios y agrupaciones de almacenamiento
Puede optimizar la eficiencia de su solución de cinta no mezclando formatos de medios en una misma agrupación de almacenamiento. En lugar de mezclar distintos formatos, correlacione cada formato de medio con una agrupación de almacenamiento distinta utilizando su propia clase de dispositivo. Esta restricción también se aplica a los formatos LTO.

Diferentes generaciones de medios en una biblioteca

El servidor de IBM Spectrum Protect permite mezclar tipos de dispositivo en una biblioteca automatizada, pero normalmente no se admite mezclar distintas generaciones del mismo tipo de unidad. Las nuevas unidades no pueden grabar en los formatos de medios más antiguos y las unidades antiguas no pueden leer los formatos nuevos. Las unidades LTO Ultrium no son una excepción a esta regla.

Si la tecnología de unidad nueva no puede grabar en medios que se hayan formateado con unidades de generaciones anteriores, los medios más antiguos deben marcarse como de sólo lectura para evitar problemas en las operaciones de servidor. Asimismo, las unidades más antiguas deben retirarse de la biblioteca, o bien del servidor. Por ejemplo, el servidor de IBM Spectrum Protect no admite el uso de unidades Oracle StorageTek 9940A con unidades 9940B en combinación con otros tipos de dispositivos en una misma biblioteca.

En general, IBM Spectrum Protect no admite mezclar distintas generaciones de unidades y medios LTO Ultrium. No obstante, se admiten las mezclas siguientes:

- LTO Ultrium Generación 3 (LTO-3) con LTO Ultrium Generación 4 (LTO-4)
- LTO Ultrium Generación 4 (LTO-4) con LTO Ultrium Generación 5 (LTO-5)
- LTO Ultrium Generación 5 (LTO-5) con LTO Ultrium Generación 6 (LTO-6)
- LTO Ultrium Generación 6 (LTO-6) con LTO Ultrium Generación 7 (LTO-7)

El servidor admite estas mezclas porque las distintas unidades pueden leer y grabar en medios diferentes. Si tiene previsto actualizar todas las unidades a generación 4 (o generación 5, 6 o 7), debe suprimir todas las definiciones de unidades LTO Ultrium existentes y las vías de acceso asociadas a las mismas. A continuación, puede definir las nuevas unidades y vías de acceso para Generación 4 (o Generación 5, 6, o 7).

Restricciones que se aplican a una combinación de medios y unidades de cinta LTO Ultrium

- Las unidades LTO-5 solo pueden leer medios LTO-3. Si mezcla unidades y medios LTO-3 con unidades y medios LTO-5 en una única biblioteca, deberá marcar los medios LTO-3 media como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-3.
- Las unidades LTO-6 solo pueden leer medios LTO-4. Si mezcla unidades y medios LTO-4 con unidades y medios LTO-6 en una sola biblioteca, deberá marcar los medios LTO-4 como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-4.
- Las unidades LTO-7 solo pueden leer medios LTO-5. Si mezcla unidades y medios LTO-5 con unidades y medios LTO-7 en una sola biblioteca, deberá marcar los medios LTO-5 como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-5.

Restricciones que se aplican a unidades de cinta LTO Ultrium de mezcla de generaciones en una biblioteca

Debe utilizar cartuchos de cinta que sean una generación anterior a la unidad de cinta. Una unidad de cinta de generación posterior puede leer y grabar datos en un cartucho de cinta de generación anterior. Por ejemplo, si una biblioteca tiene unidades de cinta LTO-7 y LTO-6, debe utilizar cartuchos de cinta LTO-6. Tanto las unidades de cinta LTO-7 como LTO-6 pueden leer y grabar datos en cartuchos de cinta LTO-6.

Restricciones que se aplican a cartuchos de cinta LTO Ultrium de mezcla de generaciones en una biblioteca

Debe utilizar un cartucho de cinta que sea de la misma generación que la unidad de cinta, o una generación anterior. Por ejemplo, si una biblioteca tiene unidades de cinta LTO-7, puede utilizar cartuchos de cinta LTO-7 o una combinación de

cartuchos de cinta LTO-7 y LTO-6. Si esta biblioteca tiene cartuchos de cinta LTO-7, LTO-6 y LTO-5, debe cambiar el modo de acceso a READONLY para los cartuchos de cinta LTO-5.

Para obtener más información sobre consideraciones adicionales al mezclar generaciones de LTO Ultrium, consulte Definición de las clases de dispositivo LTO.

Cuando utilice IBM Spectrum Protect, no puede mezclar unidades que sean 3592, TS1130, TS1140, TS1150, ni generaciones de unidades posteriores. Utilice una de las tres configuraciones especiales. Para obtener información detallada al respecto, consulte el apartado Definición de clases de dispositivo 3592.

Si tiene previsto cifrar volúmenes en una biblioteca, no mezcle las generaciones de medios en la biblioteca.

Mezcla de medios y agrupaciones de almacenamiento

Puede optimizar la eficiencia de su solución de cinta no mezclando formatos de medios en una misma agrupación de almacenamiento. En lugar de mezclar distintos formatos, correlacione cada formato de medio con una agrupación de almacenamiento distinta utilizando su propia clase de dispositivo. Esta restricción también se aplica a los formatos LTO.

Varias agrupaciones de almacenamiento y sus clases de dispositivo de distintos tipos pueden apuntar a la misma biblioteca que puede admitirlos, tal como se describe en Diferentes generaciones de medios en una biblioteca.

Puede migrar a una nueva generación de tipos de soporte dentro de la misma agrupación de almacenamiento realizando los pasos siguientes:

1. Sustituya todas las unidades más antiguas por las unidades de generaciones más recientes dentro de la biblioteca. Las unidades se deben mezclar.
2. Marque los volúmenes existentes con los formatos más antiguos como de sólo lectura si la nueva unidad no puede añadir esas cintas en el formato antiguo. Si la nueva unidad puede grabar en los medios existentes en su formato antiguo, este paso no es necesario, aunque el Paso 1 sí lo es. Si es necesario mantener varias generaciones de unidades diferentes que se pueden leer pero no grabar dentro de la misma biblioteca, utilice agrupaciones de almacenamiento diferentes.




Definiciones necesarias para dispositivos de almacenamiento en cinta



Para que el servidor de IBM Spectrum Protect pueda utilizar un dispositivo de cinta, debe configurar el dispositivo en el sistema operativo y en el servidor. Durante el proceso de planificación, determine qué definiciones se necesitan para sus dispositivos de almacenamiento en cinta.


Consejo: Puede utilizar el mandato PERFORM LIBACTION para simplificar el proceso en el que añade dispositivos a los tipos de biblioteca SCSI y VTL.

La Tabla 1 resume las definiciones obligatorias para diferentes tipos de dispositivos.

Tabla 1. Definiciones necesarias para los dispositivos de almacenamiento

Dispositivo	Tipos de dispositivo	Definiciones necesarias			
		Biblioteca	Unidad	Vía de acceso	Clase de dispositivo
Disco magnético	DISK	—	—	—	Sí ¹
	FILE ²	—	—	—	Sí
	 Sistemas operativos AIX  Sistemas operativos Windows CENTERA  Sistemas operativos LinuxCENTERA ³	—	—	—	Sí

Dispositivo	Tipos de dispositivo	Definiciones necesarias			
		Biblioteca	Unidad	Vía de acceso	Clase de dispositivo
Cinta	<ul style="list-style-type: none"> • 3590 • 3592 • DLT • LTO • NAS • VOLSAFE  Sistemas operativos AIX  Sistemas operativos Windows GENERICTAPE ECARTRIDGE ⁴	Sí	Sí	Sí	Sí
Medios extraíbles (sistema de archivos)	REMOVABLEFILE	Sí	Sí	Sí	Sí


1. La clase de dispositivo DISK ya existe en el momento de la instalación y no se puede modificar.
2. Se requieren bibliotecas, unidades y vías de acceso FILE para compartir con los agentes de almacenamiento.
3.  Sistemas operativos Linux El tipo de dispositivo CENTERA está disponible solo para sistemas Linux x86_64.
4. El tipo de dispositivo ECARTRIDGE es para unidades de cinta de cartucho Oracle StorageTek como unidades 9840 y T10000.

Planificación de la jerarquía de agrupaciones de almacenamiento

Planifique la jerarquía de agrupaciones de almacenamiento para asegurarse de que los datos se migran a diario de disco a cinta. La migración libera espacio en el dispositivo de disco y mueve los datos a la cinta para la retención a largo plazo. De esta manera, podrá aprovechar la escalabilidad, la rentabilidad y las características de seguridad del almacenamiento de cintas.

Antes de empezar

La jerarquía de agrupaciones de almacenamiento ayuda a gestionar el flujo de datos. Para comprender el flujo de datos, revise Figura 1. Figura 1. Solución de cinta



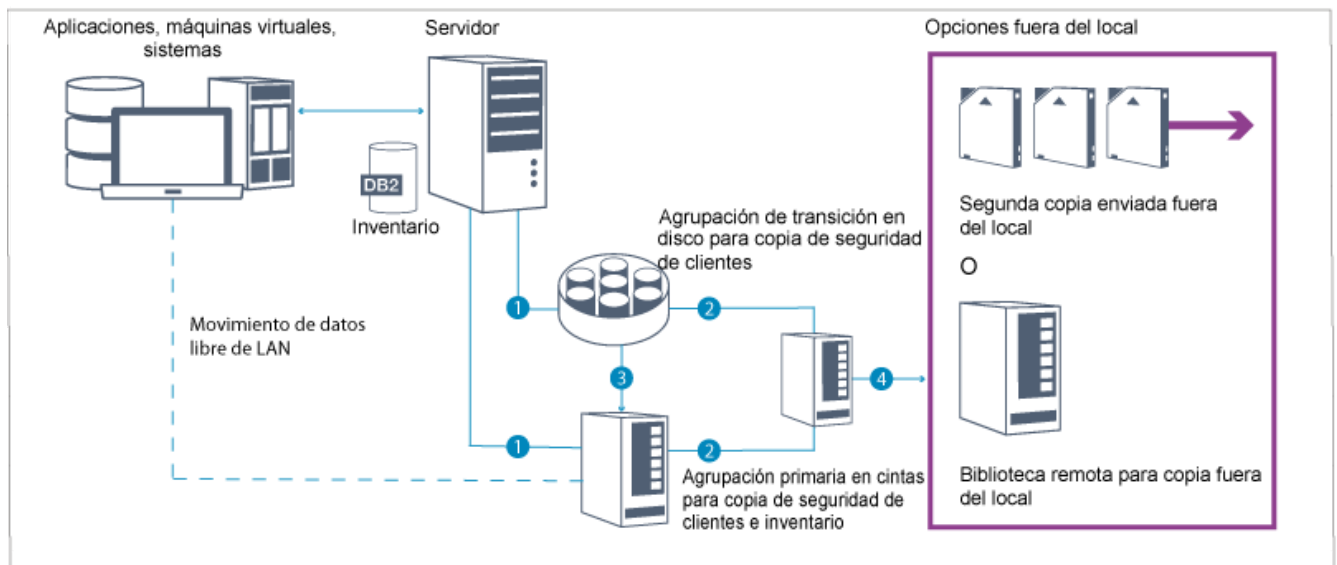
Cinta

✔ Ideal para retención a largo plazo

✔ Escalabilidad a bajo coste

✔ Zona de transición disco a agrup. cintas

✔ Optimizado para SAN



Los pasos siguientes corresponden a los números de la figura:

1. El servidor recibe datos de los clientes (aplicaciones, máquinas virtuales o sistemas) y almacena los datos en agrupaciones de almacenamiento primaria. En función del tipo de cliente, los datos se almacenan en una agrupación de almacenamiento primaria

- en disco o cinta.
- 2. La copia de seguridad de los datos en disco y cinta se realiza en una agrupación de almacenamiento de copias en cinta.
- 3. Los datos de la agrupación de almacenamiento primario en disco se migran a diario a la agrupación de almacenamiento primario en cinta.
- 4. Los datos de la agrupación de almacenamiento de copias en cinta se mueva fuera de local para dar soporte a la retención a largo plazo y a la recuperación tras desastre.

Procedimiento

Para planificar la jerarquía de agrupaciones de almacenamiento, responda a las siguientes preguntas:

- a. ¿Qué clientes deben realizar copias de seguridad de los datos en discos, y qué clientes en cinta?
 - o El método preferido es realizar una copia de seguridad de los clientes que alojan objetos grandes, como bases de datos, en cinta.
 - o El método preferido es realizar una copia de seguridad de todos los demás clientes en el disco.
 - o La copia de seguridad de los clientes de máquina virtual (VM) se puede realizar en disco o cinta. El método preferido es realizar una copia de seguridad de un cliente de máquina virtual en una agrupación de almacenamiento de disco independiente, que no se migra a cinta. Si tiene que migrar un cliente de máquina virtual en cinta, cree una agrupación de almacenamiento de disco más pequeña para albergar los archivos de control de VMware. Esta agrupación de almacenamiento de disco más pequeña no se puede migrar a cinta. Para obtener más información sobre cómo hacer copia de seguridad de un cliente de máquina virtual en cinta, consulte Directrices del soporte de cinta y nota técnica 1239546.

Consejo: Si muchos clientes tienen que realizar la copia de seguridad de datos en una única agrupación de almacenamiento, considere la posibilidad de utilizar una agrupación de almacenamiento en disco porque puede especificar muchos puntos de montaje. Puede especificar un valor máximo de 999 para el parámetro MAXNUMMP en el mandato REGISTER NODE.

- b. ¿Cuáles son las consideraciones para especificar la capacidad de las agrupaciones de almacenamiento basadas en disco?

Como mínimo, planifique suficiente capacidad para almacenar datos de un único día de operaciones de copia de seguridad. El método preferido es planificar capacidad suficiente para almacenar datos de dos días de operaciones de copia de seguridad y añadir un 20% de almacenamiento intermedio.

- c. ¿Cuáles son las consideraciones para especificar la clase de dispositivo para la agrupación de almacenamiento basada en disco?

El método preferido es especificar una clase de dispositivo FILE. Establezca el parámetro MOUNTLIMIT en 4000. Asegúrese también de que el nodo tenga un número lo suficientemente alto de puntos de montaje, que podrá especificar utilizando el parámetro MAXNUMMP en el mandato REGISTER NODE.

- d. ¿Debe especificarse la deduplicación de datos para la agrupación de almacenamiento de disco?

No, porque los datos se almacenan en el disco sólo un día antes de que los datos se migren a cinta.

- e. ¿Debe especificarse la migración automática de datos en base al umbral de migración?

No. En cambio, planifique una migración diaria utilizando el mandato MIGRATE STGPOOL. (para impedir la migración automática basada en el umbral de migración, especifique un valor de 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG cuando emita el mandato DEFINE STGPOOL.)

- f. ¿Debe especificarse un retardo en la migración?

El método preferido consiste en especificar la migración desde el disco a la cinta a diario, y no especificar un retardo de migración, lo que requiere planificación adicional. Para obtener más información sobre retardos en la migración, consulte Migración de archivos en una jerarquía de agrupaciones de almacenamiento.

- g. ¿Cómo se puede calcular el número de unidades de cinta?

- i. Determine la velocidad de transferencia de datos nativos de la unidad revisando la documentación del fabricante. Para obtener un cálculo aproximado de la velocidad de transferencia de datos constante en el entorno de almacenamiento, reste el 30% de la velocidad de transferencia de datos nativos.
- ii. Calcule la velocidad necesaria de la ingestión de datos por el servidor. A continuación, divida esta cifra entre la velocidad de transferencia de datos constante de un único dispositivo de cinta. El resultado es el número mínimo de unidades para dar soporte a la ingestión de datos.
- iii. Calcule el número de puntos de montaje necesarios por los clientes que realizan la copia de seguridad de datos en cinta, incluyendo aquellos clientes que utilizan varias sesiones. Puede distribuir los puntos de montaje a través de la ventana de copia de seguridad, teniendo en cuenta que es probable que los clientes realicen copias de seguridad de objetos de gran tamaño, que pueden utilizar la mayoría de la ventana.
- iv. Calcular los requisitos de rendimiento y puntos de montaje que son necesarios para tareas de mantenimiento, como la migración de disco a cinta y las copias de cinta a cinta. Al realizar la copia de seguridad de datos a cinta, puede evitar el proceso de migración pero realizar copias de cinta a cinta doblará el requisito de unidad de cintas.

- v. Calcule el número de unidades adicionales que pueden necesitarse, por ejemplo:
- Si una unidad de cintas funciona mal, el problema afectará al número de puntos de montaje disponibles y a la velocidad de ingestión. Considere el suministro de unidades de repuesto. Por ejemplo, si necesita cinco unidades de cinta para las operaciones normales, considere el suministro de dos unidades de repuesto.
 - Las operaciones de restauración y recuperación pueden requerir unidades de cinta adicionales si tiene previsto ejecutar las operaciones simultáneamente con la ingestión de datos y las operaciones de mantenimiento. Si es necesario, suministre unidades de cinta adicionales y asegúrese de que no se utilicen cuando inicie las operaciones de restauración o recuperación.
- h. ¿Qué alternativas están disponibles para optimizar las operaciones de restauración?
- Puede utilizar la función de proximidad para mejorar el rendimiento del sistema y optimizar la organización de datos. La función de proximidad puede reducir el número de volúmenes a los que se debe acceder cuando debe restaurarse una gran cantidad de datos:
- Para agrupaciones de almacenamiento basadas en disco, el método preferido es utilizar la función de proximidad por nodo. El servidor almacena los datos del nodo en el menor número posible de volúmenes.
 - Para agrupaciones de almacenamiento basadas en cinta, el método preferido es utilizar la función de proximidad por grupo. La proximidad por grupo genera una reducción de la capacidad de cinta no utilizada, lo que permite más datos colocados en cintas individuales.

Para obtener más información sobre la función de proximidad, consulte Optimización de operaciones habilitando la función de proximidad de los archivos de cliente.

Si es un administrador del sistema con experiencia, es posible que tenga previstas acciones adicionales para optimizar las operaciones de restauración. Consulte Optimización de las operaciones de restauración para clientes, Técnicas de copia de seguridad de archivo y MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial).

Almacenamiento de datos fuera del local

Para facilitar la recuperación de datos y como parte de la estrategia de recuperación tras desastre, almacene copias de cinta fuera del local.

Utilice la función del gestor recuperación tras desastre (DRM) para configurar y generar automáticamente un plan de recuperación tras desastre que contenga la información, los scripts y los procedimientos necesarios para restaurar automáticamente los datos del cliente de recuperación y servidor tras un desastre. Elija entre una de las siguientes opciones de almacenamiento de datos fuera del local como estrategia de recuperación tras desastre para proteger las copias de cinta:

Cámaras de seguridad fuera del local desde un único sitio de producción

Volúmenes de almacenamiento, como cartuchos de cinta y volúmenes de soporte, se guardan en una cámara de seguridad fuera del local. Un transportista transporta los datos desde una instalación de almacenamiento fuera del local al sitio de recuperación. Si se produce un desastre, los volúmenes se vuelven a enviar al sitio de producción una vez restaurados el hardware y el servidor de IBM Spectrum Protect.

Cámaras de seguridad fuera del local con un sitio de recuperación

Un transportista mueve volúmenes de almacenamiento desde el sitio de producción hasta una instalación de almacenamiento fuera del local. Al implantar un sitio de recuperación dedicado, puede reducir el tiempo de recuperación, en comparación con un único sitio de producción. Sin embargo, esta opción incrementa el coste de la recuperación tras desastre porque debe mantenerse más hardware y software. Por ejemplo, el sitio de recuperación debe tener dispositivos de cinta compatibles y el software del servidor de IBM Spectrum Protect. Para poder recuperar el sitio de producción, el hardware y el software en el sitio de recuperación deben estar configurados y en ejecución.

Cámara de seguridad electrónica

Para utilizar la cámara de seguridad electrónica como estrategia de recuperación tras desastre, el sitio de recuperación debe tener un servidor IBM Spectrum Protect en ejecución. Los datos críticos se guardan en una cámara de seguridad electrónica desde el sitio de producción hasta el sitio de recuperación. DRM también se utiliza para el almacenamiento en cámaras de seguridad fuera del local de datos no críticos. La cámara de seguridad electrónica mueve los datos críticos fuera del local más rápidamente y con más frecuencia que los métodos de transportista tradicional. El tiempo de recuperación se reduce porque los datos críticos ya están almacenados en el sitio de recuperación. Sin embargo, como el sitio de recuperación se ejecuta de forma continua, el coste de la estrategia de recuperación tras desastre es más caro que el almacenamiento en cámaras de seguridad fuera del local.

Conceptos relacionados:

Preparación ante desastres y recuperación tras desastres mediante DRM

Planificación de la seguridad

Planee proteger la seguridad de los sistemas en la solución IBM Spectrum Protect con controles de acceso y autenticación y tenga en cuenta el cifrado de datos y la transmisión de contraseña.

- Planificación de los roles de administración
Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.
- Planificación para comunicaciones seguras
Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.
- Planificación de almacenamiento de datos cifrados
Determine si la compañía requiere que se cifren los datos almacenados y elija el método que mejor se adapta a sus necesidades.
- Planificación del acceso de cortafuegos
Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Planificación de los roles de administración

Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.

Puede asignar uno de los siguientes niveles de autorización a los administradores:

Sistema

Los administradores con autoridad del sistema tienen el nivel de autorización más alto. Los administradores con este nivel pueden realizar cualquier tarea. Pueden gestionar todos los dominios de política y agrupaciones de almacenamiento y otorgar autoridad a otros administradores.

Política

Los administradores que tienen autorización sobre políticas pueden gestionar todas las tareas relacionadas con la gestión de políticas. Este privilegio puede no tener restricciones o puede estar restringido a dominios de políticas específicos.

Almacenamiento

Los administradores que tienen autorización de almacenamiento pueden asignar y controlar recursos de almacenamiento para el servidor.

Operador

Los administradores que tienen autorización de operador pueden controlar la operación inmediata del servidor y la disponibilidad de soporte de almacenamiento como unidades y bibliotecas de cintas.

Los escenarios de Tabla 1 proporcionan ejemplos de por qué es posible que desee asignar distintos niveles de autorización para que los administradores puedan realizar tareas:

Tabla 1. Escenarios para roles de administrador

Escenario	Tipo de ID de administrador a configurar
Un administrador de una pequeña empresa gestiona el servidor y es responsable de todas las actividades del servidor.	<ul style="list-style-type: none"> • Autoridad del sistema: 1 ID de administrador
Un administrador para varios servidores también gestiona el sistema en general. Otros diversos administradores gestionan sus propias agrupaciones de almacenamiento.	<ul style="list-style-type: none"> • Autoridad del sistema en todos los servidores: 1 ID de administrador para el administrador del sistema general • Autoridad de almacenamiento para agrupaciones de almacenamiento designadas: 1 ID de administrador para cada uno de los otros administradores
Un administrador gestiona 2 servidores. Otra persona ayuda con las tareas de administración. Dos ayudantes son responsables de ayudar a garantizar que se hace copia de seguridad de los sistemas importantes. Cada ayudante es responsable de supervisar las copias de seguridad planificadas en uno de los servidores de IBM Spectrum Protect.	<ul style="list-style-type: none"> • Autoridad del sistema en ambos servidores: 2 ID de administrador • Autoridad de operador: 2 ID de administrador para los ayudantes con acceso al servidor del que cada persona es responsable

Tareas relacionadas:

Gestión de administradores

Planificación para comunicaciones seguras

Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.

Determine el nivel de protección necesario para los datos, basándose en las regulaciones y requisitos empresariales bajo los que opera la compañía.

Si su empresa necesita un alto nivel de seguridad para las contraseñas y la transmisión de datos, planea implementar comunicaciones seguras con protocolos de seguridad de la capa de transporte (TLS) o de capa de sockets seguros (SSL).

TLS y SSL proporcionan comunicaciones seguras entre el servidor y el cliente, pero pueden afectar al rendimiento del sistema. Para mejorar el rendimiento del sistema, utilice TLS para autenticarse sin cifrar datos de objetos. Para especificar si el servidor debe utilizar TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor y el parámetro UPDATE SERVER=SSL para la comunicación de servidor a servidor. A partir de la versión V8.1.2, se utiliza TLS para la autenticación predeterminada. Si decide utilizar TLS para cifrar sesiones enteras, utilice el protocolo solo para las sesiones en las que es necesario y añada recursos de procesador en el servidor para gestionar el incremento del tráfico de red. También puede probar otras opciones. Por ejemplo, algunos dispositivos, como los direccionadores o los conmutadores, proporcionan la función TLS o SSL.

Puede utilizar TLS y SSL para proteger todas o algunas de las distintas vías de acceso de comunicación posibles, por ejemplo:

- Centro de operaciones: De navegador a concentrador; de concentrador a radio
- Cliente a servidor
- Servidor a servidor: réplica de nodo en el servidor:

Tareas relacionadas:

Configuración de comunicaciones seguras con Seguridad de la capa de transporte

Planificación de almacenamiento de datos cifrados

Determine si la compañía requiere que se cifren los datos almacenados y elija el método que mejor se adapta a sus necesidades.

Tabla 1. Selección de un método de cifrado de datos

Requisito empresarial	Método de cifrado	Información adicional
Proteger los datos a nivel de cliente.	Cifrado del cliente de IBM Spectrum Protect	Puede cifrar los datos al nivel de archivos utilizando una lista de inclusión/exclusión. De este modo, puede mantener un alto grado de control sobre los datos que estén cifrados. Se necesitan recursos informáticos adicionales en el cliente que pueden afectar al rendimiento de los procesos de copia de seguridad y restauración. Para obtener más información acerca de este método, consulte Cifrado de cliente de IBM Spectrum Protect.
Proteger los datos de volúmenes de agrupación de almacenamiento en una unidad de cintas.	Método de aplicación	Cuando se utiliza el método de aplicaciones, IBM Spectrum Protect gestiona las claves de cifrado para proteger los datos de los volúmenes de agrupación de almacenamiento. Preste especial atención para proteger las copias de seguridad de las bases de datos porque las claves de cifrado se almacenan en la base de datos del servidor. Si no dispone de acceso a las copias de seguridad de la base de datos y a las claves de cifrado coincidentes, no podrá restaurar los datos. No puede utilizar este método para cifrar copias de seguridad de bases de datos, datos exportados o conjuntos de copias de seguridad. Para obtener más información sobre el método Aplicación, consulte Métodos de cifrado de cinta.
Proteger los datos en una unidad de cintas.	Método de biblioteca	Cuando se utiliza el método Biblioteca, la biblioteca gestiona las claves de cifrado. Puede cifrar los datos de las agrupaciones de almacenamiento y otros datos en una unidad de cintas. Puede controlar qué volúmenes se cifran utilizando sus números de serie de código de barras. Para obtener más información sobre el método Biblioteca, consulte Métodos de cifrado de cinta.
Proteger los datos en una unidad de cintas.	Método de sistema	Cuando utilice el método Sistema, un controlador de dispositivo o el sistema operativo AIX gestiona el cifrado. Este método de cifrado sólo está disponible en el sistema operativo AIX. Puede cifrar los datos de las agrupaciones de almacenamiento y otros datos en una unidad de cintas. Para obtener más información sobre el método Sistema, consulte Métodos de cifrado de cinta.

Planificación del acceso de cortafuegos

Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Tabla 1 describe los puertos utilizados por el servidor, el cliente y el Centro de operaciones.

Tabla 1. Puertos utilizados por el servidor, el cliente y Centro de operaciones

Elemento	Valor predeterminado	Dirección	Descripción
----------	----------------------	-----------	-------------

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (TCPPOINT)	1500	Entrada/salida	Cada instancia de servidor necesita un puerto exclusivo. Puede especificar un número de puerto alternativo. La opción TCPPOINT realiza escuchas para sesiones habilitadas para TCP/IP y SSL desde el cliente. Puede utilizar la opción TCPADMINPORT y la opción ADMINONCLIENTPORT para establecer los valores de puerto para el tráfico de cliente administrativo.
Puerto solo SSL (SSLTCPPOINT)	No tiene valor predeterminado	Entrada/salida	Este puerto se utiliza si desea restringir la comunicación en el puerto a sesiones solo habilitadas para SSL. Un servidor puede soportar las comunicaciones SSL y no SSL utilizando las opciones TCPPOINT o TCPADMINPORT.
SMB	45	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.
Réplica	No tiene valor predeterminado	Entrada/salida	El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica. Los puertos de entrada para la réplica son los puertos TCP y SSL que están especificados para el servidor de origen en el mandato DEFINE SERVER.
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesiones de larga ejecución	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente/servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	Si tiene previsto utilizar servicios de gestión de cliente de IBM Spectrum Protect, el puerto servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

Tareas relacionadas:

➤ Recopilación de información de diagnóstico con servicios de gestión de cliente de IBM Spectrum Protect

Referencia relacionada:

➤ ADMINONCLIENTPORT, opción de servidor

➤ DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

➤ TCPADMINPORT, opción de servidor

➤ TCPPOINT, opción de servidor

Implementación de una solución de protección de datos basada en cinta

Implemente la solución basada en cinta, que utiliza copia de seguridad 'de disco a disco a cinta' y disco intermedio para optimizar el almacenamiento. Al implementar la solución de cinta, puede habilitar la retención de datos a largo plazo y lograr una escalabilidad de bajo coste.



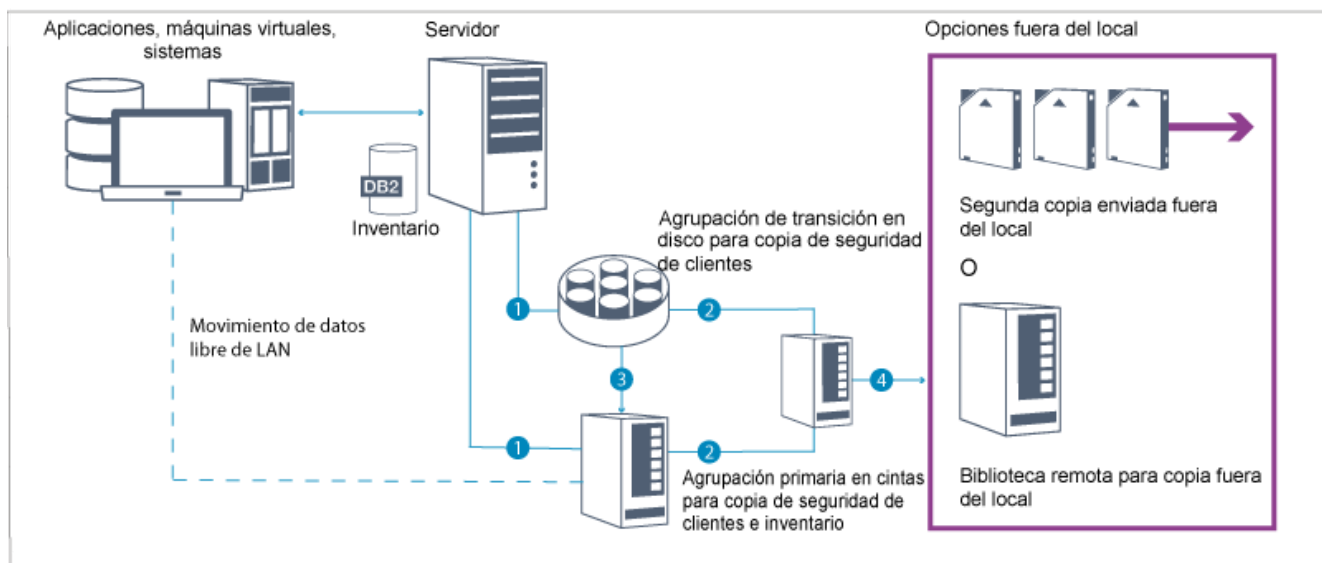
Cinta

✓ Ideal para retención a largo plazo

✓ Escalabilidad a bajo coste

✓ Zona de transición disco a agrup. cintas

✓ Optimizado para SAN



Consejo: La solución descrita no incluye réplica de nodo. Sin embargo, si quiere utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento de disco a disco, asegúrese de que la operación de réplica esté completada antes de migrar los datos de disco a disco. También puede utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento en un dispositivo de cinta local a una agrupación de almacenamiento de copia en un dispositivo de cinta local.

Hoja de ruta de la implementación

Se requieren los siguientes pasos para configurar una solución basada en cinta.

1. Configurar el sistema.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
4. Conectar dispositivos de cinta para el servidor.
5. Configurar bibliotecas de cintas para su uso por parte de un servidor.
6. Configurar una jerarquía de agrupaciones de almacenamiento.
7. Instalar y configurar clientes.
8. Configurar el movimiento de datos sin LAN.
9. Seleccionar un método de cifrado y configurar el cifrado.
10. Definir operaciones de almacenamiento en cinta.
11. Completar la implementación.

Configuración del sistema

Para configurar el sistema, primero debe configurar el hardware de almacenamiento de disco y el sistema servidor para IBM Spectrum Protect.

Acerca de esta tarea

Consejo: Se describen los procedimientos para configurar el sistema de almacenamiento de disco y servidor. Para empezar a configurar dispositivos de cinta, consulte Conexión de dispositivos de cinta para el servidor.

- Configuración del hardware de almacenamiento
Para optimizar el almacenamiento de disco, revise las directrices para configurar el almacenamiento de disco con IBM Spectrum Protect. A continuación, proporcione una conexión entre el servidor y los dispositivos de almacenamiento de disco y complete otras tareas de configuración.
- Instalación del sistema operativo del servidor
Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Configuración de E/S de la multivía de acceso puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.
- Creación del ID de usuario para el servidor
Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.
- Preparación de sistemas de archivos para el servidor
Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

Configuración del hardware de almacenamiento

Para optimizar el almacenamiento de disco, revise las directrices para configurar el almacenamiento de disco con IBM Spectrum Protect. A continuación, proporcione una conexión entre el servidor y los dispositivos de almacenamiento de disco y complete otras tareas de configuración.

Antes de empezar

Para obtener directrices sobre cómo configurar el almacenamiento en disco, consulte Lista de comprobación para agrupaciones de almacenamiento en DISK o FILE

Procedimiento

1. Proporcione una conexión entre el servidor y los dispositivos de almacenamiento siguiendo estas directrices:
 - Utilice un conmutador o conexión directa para las conexiones de canal de fibra.
 - Tenga en cuenta el número de puertos que están conectados y la cantidad de ancho de banda que se necesita.
 - Tenga en cuenta el número de puertos en el servidor y el número de puertos de host en el sistema de discos que están conectados.
2. Verifique que los controladores de dispositivo y firmware para el sistema servidor, adaptadores y sistema operativo son actuales y están en los niveles recomendados.
3. Configure matrices de almacenamiento. Asegúrese de que ha planificado correctamente para garantizar un rendimiento óptimo. Para obtener más información, consulte Planificación del almacenamiento en disco.
4. Asegúrese de que el sistema servidor tiene acceso a los volúmenes de disco que se han creado. Realice los pasos siguientes:
 - a. Si el sistema está conectado a un conmutador de canal de fibra, divida el servidor por zonas para ver los discos.
 - b. Correlacione todos los volúmenes para indicar al sistema de discos que este servidor específico está autorizado para ver cada disco.
5. Asegúrese de que los dispositivos de cinta y de disco utilicen distintos puertos de adaptador de bus de host (HBA). Controle la E/S de disco y cinta utilizando la SAN.

Tareas relacionadas:

Configuración de E/S de la multivía de acceso

Instalación del sistema operativo del servidor

Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Instalación en sistemas AIX
Complete los pasos siguientes para instalar AIX en el sistema servidor.
- Instalación en sistemas Linux
Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.
- Instalación en sistemas Windows
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

Instalación en sistemas AIX

Complete los pasos siguientes para instalar AIX en el sistema servidor.

Procedimiento

1. Instale AIX Versión 7.1, TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Habilite los puertos de terminación de E/S de AIX emitiendo el siguiente mandato:

```
chdev -l iocp0 -P
```

El rendimiento de servidor puede verse afectado por la definición de huso horario de Olson.

5. Para optimizar el rendimiento, cambie el formato de huso horario del sistema de Olson a POSIX. Utilice el siguiente formato de mandato para actualizar el valor de huso horario:

```
chtz=local_timezone,date/time,date/time
```

Por ejemplo, si ha vivido en Tucson, Arizona, donde se utiliza la franja horaria de las Rocosas, deberá emitir el siguiente mandato para cambiar el formato POSIX:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Añada una entrada en el `.profile` del usuario de la instancia para que se defina el entorno siguiente:

```
export MALLOCOPTIONS=multiheap:16
```

7. Defina el sistema para crear archivos principales de aplicación completos. Emita el mandato siguiente:

```
chdev -l sys0 -a fullcore=true -P
```

8. Para las comunicaciones con el servidor y Centro de operaciones, asegúrese de que los siguientes puertos están abiertos en todos los cortafuegos que puedan existir:

- Para las comunicaciones con el servidor, abra el puerto 1500.
- Para las comunicaciones seguras con Centro de operaciones, abra el puerto 11090 en el servidor concentrador.

Si no utiliza los valores de puerto predeterminados, asegúrese de que los puertos que está utilizando están abiertos.

9. Habilite las mejoras de alto rendimiento de TCP. Emita el mandato siguiente:

```
no -p -o rfc1323=1
```

10. Para obtener una fiabilidad y un rendimiento óptimos, vincule cuatro puertos Ethernet de 10 Gb. Utilice la herramienta de la interfaz de gestión del sistema (SMIT) para vincular los puertos utilizando Etherchannel. Durante las pruebas se utilizaron los siguientes valores:

mode	8023ad	
auto_recovery	yes	Habilitar la recuperación automática tras la migración tras error.
backup_adapter	NONE	Adaptador utilizado cuando falla todo el canal.
hash_mode	src_dst_port	Determina cómo se elige el adaptador saliente.
interval	long	Determina el valor de intervalo para IEEE.
mode	8023ad	Modalidad de 802.3ad
		Modalidad de funcionamiento de EtherChannel
netaddr	0	Dirección para el ping
no_loss_failover	yes	Habilitar migración tras error sin pérdidas tras anomalía del ping
num_retries	3	Veces que reintentar el ping antes de considerarlo un error
retry_time	1	Tiempo de espera (en segundos) entre pings
use_alt_addr	no	Habilitar dirección EtherChannel alternativa
use_jumbo_frame	no	Habilitar tramas de gran tamaño de Gigabit Ethernet

11. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 1. Si los valores `ulimit` no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 1. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	ulimit -Hc
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	ulimit -Hd
Tamaño de archivo máximo	fsize	Ilimitado	ulimit -Hf
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.

Antes de empezar

El sistema operativo se instalará en los discos duros internos. Configure los discos duros internos utilizando una matriz de hardware de RAID 1. Por ejemplo, si está configurando un sistema pequeño, los dos discos internos de 300 GB se duplican en RAID 1 de modo que aparece disponible un único disco de 300 GB para el instalador del sistema operativo.

Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
 - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
 - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
 - c. Seleccione las preferencias de idioma y teclado.
 - d. Seleccione la ubicación para establecer el huso horario correcto.
 - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
 - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:
 - El disco local de 300 GB se ha seleccionado como destino de instalación.
 - En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.
 Pulse Terminado.
 - g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root. Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato df para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

```
[root@tvapp02]# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root     50G  3.0G  48G   6% /
devtmpfs                  32G   0    32G   0% /dev
tmpfs                     32G   92K   32G   1% /dev/shm
tmpfs                     32G   8.8M   32G   1% /run
tmpfs                     32G   0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home    220G   37M  220G   1% /home
/dev/sda1                 497M  124M  373M  25% /boot
```

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agrega varios puertos subordinados a una sola conexión lógica. El método preferido es utilizar una modalidad de vínculo de 802.3ad, un valor de miimon de 100 y un valor de xmit_hash_policy de layer3+4.

Restricción: Para utilizar una conexión de red LACP, debe disponer de un conmutador de red que admita LACP.

Para obtener instrucciones adicionales sobre cómo configurar conexiones de red vinculadas con Red Hat Enterprise Linux Versión 7, consulte Crear una interfaz de acoplamiento de canal.

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Instale los componentes que son necesarios para la instalación de servidor. Complete los pasos siguientes para crear un repositorio Yellowdog Updater Modified (YUM) e instale los paquetes de requisitos previos.

- a. Monte el DVD de instalación de Red Hat Enterprise Linux en el directorio del sistema. Por ejemplo, para montarlo en el directorio `/mnt`, emita el siguiente mandato:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Verifique que el DVD se ha montado emitiendo el mandato `mount`. Debería ver una salida similar al ejemplo siguiente:

```
/dev/sr0 on /mnt type iso9660
```

- c. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

Si el directorio `repos.d` no existe, créelo.

- d. Liste el contenido de directorio:

```
ls rhel-source.repo
```

- e. Cambie el nombre del archivo `repo` original emitiendo el mandato `mv`. Por ejemplo:

```
mv rhel-source.repo rhel-source.repo.orig
```

- f. Cree un nuevo archivo `repo` utilizando un editor de texto. Por ejemplo, para utilizar el editor `vi`, emita el siguiente mandato:

```
vi rhel71_dvd.repo
```

- g. Añada las líneas siguientes al nuevo archivo `repo`. El parámetro `baseurl` especifica el punto de montaje del directorio:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

- h. Instale el paquete de requisito previo `ksh.x86_64`, emitiendo el mandato `yum`. Por ejemplo:

```
yum install ksh.x86_64
```

Excepción: No necesita instalar las bibliotecas `compat-libstdc++-33-3.2.3-69.el6.i686` y `libstdc++-i686` para Red Hat Enterprise Linux Versión 7.1.

5. Cuando se completa la instalación de software, puede restaurar los valores de repositorio YUM originales completando los pasos siguientes:

- a. Desmonte el DVD de instalación de Red Hat Enterprise Linux emitiendo el siguiente mandato:

```
umount /mnt
```

- b. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

- c. Cambie el nombre del archivo `repo` que ha creado:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Cambie el nombre del archivo original al nombre original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine si son necesarios cambios de parámetro de kernel. Realice los pasos siguientes:

- a. Utilice el mandato `sysctl -a` para listar los valores de parámetro.
- b. Analice los resultados utilizando las directrices en Tabla 1 para determinar si es necesario algún cambio.
- c. Si se necesitan cambios, establezca los parámetros en el archivo `/etc/sysctl.conf`. Los cambios de archivo se aplican cuando se inicia el sistema.

Consejo: Ajuste automáticamente los valores de parámetros de kernel y elimine la necesidad de actualizaciones manuales en estos valores. En Linux, el software de base de datos DB2 ajusta automáticamente los valores del parámetro de kernel de comunicación entre procesos (IPC) a los valores preferidos. Para obtener más información sobre los valores de parámetros de kernel, busque los parámetros de kernel de Linux en Documentación del producto IBM DB2 Versión 11.1.

Tabla 1. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción
kernel.shmmni	El número máximo de segmentos.
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes). Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas).
kernel.sem	(SEMMSL) El número máximo de semáforos por matriz.
Hay cuatro valores para el parámetro kernel.sem.	(SEMMNS) El número máximo de semáforos por sistema.
	(SEMOPM) El número máximo de operaciones por llamada a semáforo.
	(SEMMNI) El número máximo de matrices.
kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema.
kernel.msgmax	Tamaño máximo de los mensajes (bytes).
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes).
kernel.randomize_va_space	El parámetro <code>kernel.randomize_va_space</code> configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.
vm.swappiness	El parámetro <code>vm.swappiness</code> define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.
vm.overcommit_memory	El parámetro <code>vm.overcommit_memory</code> influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.

7. Abra puertos de cortafuegos para comunicarse con el servidor. Realice los pasos siguientes:

- a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.

Emita el mandato siguiente:

```
# firewall-cmd --get-active-zones
public
interfaces: ens4f0
```

b. Para utilizar la dirección de puerto predeterminada para las comunicaciones con el servidor, abra el puerto TCP/IP 1500 en el cortafuegos de Linux.

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Si desea utilizar un valor distinto del predeterminado, puede especificar un número en el rango 1024 - 32767. Si abre un puerto distinto del predeterminado, tendrá que especificar ese puerto cuando ejecute el script de configuración.

c. Si piensa utilizar este sistema como concentrador, abra el puerto 11090, que es el puerto predeterminado para las comunicaciones seguras (https).

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Vuelva a cargar las definiciones de cortafuegos para que los cambios entren en vigor.

Emita el mandato siguiente:

```
firewall-cmd --reload
```

8. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 2. Si los valores *ulimit* no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 2. Valores de los límites de usuario (*ulimit*)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	<code>ulimit -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	<code>ulimit -Hd</code>
Tamaño de archivo máximo	fsize	Ilimitado	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	nofile	65536	<code>ulimit -Hn</code>
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	<code>ulimit -Ht</code>
Número máximo de procesos de usuario	nproc	16384	<code>ulimit -Hu</code>

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

Instalación en sistemas Windows

Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

Procedimiento

1. Instale Windows Server 2016 Standard Edition, de acuerdo con las instrucciones del fabricante.
2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
 - a. Abra el editor de política de seguridad local ejecutando `secpol.msc`.
 - b. Pulse Políticas locales > Opciones de seguridad y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
 - Modo de aprobación de administrador para la cuenta de administrador integrado
 - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:
 - a. Aplique las últimas actualizaciones de Windows Server 2016.
 - b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
 - c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
 - d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.

- Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Backup server port 1500"  
dir=in action=allow protocol=TCP localport=1500
```

- En el servidor concentrador de Centro de operaciones, abra el puerto predeterminado para comunicaciones seguras (https) con Centro de operaciones. El número de puerto es 11090. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Centro de operaciones port 11090"  
dir=in action=allow protocol=TCP localport=11090
```

Configuración de E/S de la multivía de acceso

puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

- **Sistemas AIX**
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.
- **Sistemas Linux**
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.
- **Sistemas Windows**
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

Sistemas AIX

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

Procedimiento

- Determine la dirección de puerto de canal de fibra que debe utilizar para la definición de host en el subsistema de disco. Emita el mandato `lscfg` para cada puerto.

- En sistemas pequeños y medianos, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"
```

- En sistemas grandes, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"  
lscfg -vps -l fcs2 | grep "Network Address"  
lscfg -vps -l fcs3 | grep "Network Address"
```

- Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:

- `devices.common.IBM.mpio.rte`
- `devices.fcp.disk.array.rte`
- `devices.fcp.disk.rte`

- Emita el mandato `cfgmgr` para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

- Para listar los discos disponibles, emita el siguiente mandato:

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```
hdisk0 Available 00-00-00 SAS Disk Drive  
hdisk1 Available 00-00-00 SAS Disk Drive  
hdisk2 Available 01-00-00 SAS Disk Drive  
hdisk3 Available 01-00-00 SAS Disk Drive  
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk  
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk  
...
```

- Utilice la salida del mandato `lsdev` para identificar y listar ID de dispositivo para cada dispositivo de disco.

Por ejemplo, un ID de dispositivo podría ser `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

```
lspv -u
```

En un sistema IBM® Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

```
hdisk4 00f8cf083fd97327 None active
332136005076300810105780000000000003004214503IBMfcp
```

En el ejemplo, *6005076300810105780000000000030* es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

Para verificar el tamaño de disco en megabytes y compararlo con el valor que se lista para el sistema, emita el siguiente mandato:

```
bootinfo -s hdisk4
```

Sistemas Linux

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

Procedimiento

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

```
multipathconf --enable
```

Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los mandatos siguientes:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

```
multipath -l
```

4. Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan.
Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

```
[root@tapsrv01 code]# multipath -l
36005076802810c50980000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64 active undef running
| `-- 4:0:0:18 sdgb 131:112 active undef running
```

```
`-+- policy='round-robin 0' prio=0 status=enabled
|- 1:0:1:18 sdat 66:208 active undef running
`- 3:0:0:18 sddy 128:0 active undef running
```

a. Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

b. Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato `multipath -l`.

5. Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es `36005076802810c50980000000000012`.

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

Sistemas Windows

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

Procedimiento

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
2. Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan. Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

```
DEV#:      4  DEVICE NAME: Disk5 Part0  TYPE: 2145  POLICY: OPTIMIZED
SERIAL:    60050763008101057800000000000034  LUN SIZE: 2.0TB
=====
Path#      Adapter/Hard Disk  State  Mode  Select  Errors
  0        Scsi Port2 Bus0/Disk5 Part0  OPEN   NORMAL  0        0
  1        Scsi Port2 Bus0/Disk5 Part0  OPEN   NORMAL 27176    0
  2        Scsi Port3 Bus0/Disk5 Part0  OPEN   NORMAL 28494    0
  3        Scsi Port3 Bus0/Disk5 Part0  OPEN   NORMAL  0        0
```

4. Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es `60050763008101057800000000000034`

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

5. Para poner los nuevos discos en línea y borrar el atributo de 'sólo lectura', ejecute `diskpart.exe` con los mandatos siguientes. Repítalo para cada uno de los discos:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

Creación del ID de usuario para el servidor

Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.



Acerca de esta tarea

Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado (_) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:


- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Procedimiento

1. Utilice mandatos del sistema operativo para crear un ID de usuario.

-   Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

Por ejemplo, para crear el ID de usuario *tsminst1* en el grupo *tsmsrvrs* con una contraseña de *tsminst1*, emita los siguientes mandatos desde un ID de usuario de administración:


 **Sistemas operativos AIX**

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

 **Sistemas operativos Linux**

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

-  **Sistemas operativos Windows** Cree un ID de usuario y, a continuación, añada el nuevo ID al grupo de administradores. Por ejemplo, para crear el ID de usuario *tsminst1*, emita el siguiente mandato:

```
net user tsminst1 * /add
```

Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Cierre la sesión con el nuevo ID de usuario.

Preparación de sistemas de archivos para el servidor

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

- Preparación de sistemas de archivos en sistemas AIX
Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.
- Preparación de sistemas de archivos en sistemas Linux
Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.
- Preparación de sistemas de archivos en sistemas Windows
Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Preparación de sistemas de archivos en sistemas AIX

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

Procedimiento

1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos *hdiskX* disponibles. Emita los siguientes mandatos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, *hdisk0*.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato `mkvg`, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

Por ejemplo, si los nombres de dispositivo *hdisk4*, *hdisk5* y *hdisk6* corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita `lsvg` para cada grupo de volúmenes que ha creado en el paso anterior.

Por ejemplo:

```
lsvg -p tsmdb
```

La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

```
tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631      1631      327..326..326..326..326
hdisk5   active    1631      1631      327..326..326..326..326
hdisk6   active    1631      1631      327..326..326..326..326
```

4. Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato `mklv`. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco.

Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato `crfs`.

Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

```
mount -a
```

7. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado es normalmente un 1%:

```
tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks   Free      %Used    Iused    %Iused   Mounted on
/dev/tsmact00   195.12     194.59    1%        4         1%      /tsminst1/TSMalog
```


- Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios del servidor.

Preparación de sistemas de archivos en sistemas Linux

Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

- Utilizando la lista de ID de dispositivo que ha generado antes, emita el mandato mkfs para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos xfs:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Puede emitir el mandato mkfs hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

- Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato mkdir para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación.

Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
mkdir /tsminst1
```

Repita el mandato mkdir para cada sistema de archivos.

- Añada una entrada en el archivo /etc/fstab para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.

Por ejemplo:

```
/dev/mapper/36005076802810c50980000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

- Monte los sistemas de archivos que ha añadido al archivo /etc/fstab emitiendo el mandato mount -a.
- Liste todos los sistemas de archivos emitiendo el mandato df. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible. El ejemplo siguiente en un sistema IBM® Storwize muestra que la cantidad de espacio utilizado normalmente es un 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G   1% /tsminst1/TSMalog
```

- Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios del servidor IBM Spectrum Protect.

Preparación de sistemas de archivos en sistemas Windows

Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

- Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato md para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
md c:\tsminst1
```

Repita el mandato md para cada sistema de archivos.

- Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

Vaya a Gestor de servidores > Servicios de archivo y almacenamiento y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

- a. Ponga el disco en línea.
 - b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
 - c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como TSMfile00. No asigna el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como C:\tsminst1\TSMfile00.
Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.
3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato mountvol y, a continuación, revise la salida. Por ejemplo:
- ```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
C:\tsminst1\TSMdbspace00\
```
4. Una vez se ha completado la configuración de disco, reinicie el sistema.

## Qué hacer a continuación

---

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

## Instalación del servidor y Centro de operaciones

---

Utilice el asistente gráfico de IBM® Installation Manager para instalar los componentes.

- Instalación en sistemas AIX y Linux  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.
- Instalación en sistemas Windows  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

## Instalación en sistemas AIX y Linux

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.


## Antes de empezar

---

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

---


1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.  
Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.
2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package\_name* es el nombre del archivo descargado.

6.  Sistemas operativos AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:

```
lsuser
```

- De manera predeterminada, el mandato está habilitado.
7. Cambie al directorio en el que colocó el archivo ejecutable.
  8. Inicie el asistente de instalación emitiendo el mandato siguiente:

```
./install.sh
```

Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.
- Instalación de archivos RPM de requisitos previos para el asistente gráfico  
Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

## Instalación en sistemas Windows

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento

---

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM®.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Configuración del servidor y el Centro de operaciones

---

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

- Configuración de la instancia de servidor  
Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

- Instalación del cliente de archivado y copia de seguridad  
Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?
- Configuración de opciones para el servidor  
Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.
- Conceptos sobre la seguridad  
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- Configuración de Centro de operaciones  
Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.
- Registro de la licencia de producto  
Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.
- Definición de las reglas de retención de datos para su empresa  
Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.
- Definición de planificaciones para actividades de mantenimiento del servidor  
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.
- Definición de planificaciones de cliente  
Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

## Configuración de la instancia de servidor

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

### Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo sshd\_config en el directorio de /etc/ssh/. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor *localhost*.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

 Sistemas operativos Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:

1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
  - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
  - b. Seleccione Configuración avanzada.
  - c. Seleccione Reglas de entrada.
  - d. Seleccione Nueva regla.
  - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
  - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
  - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
  - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
  - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador

incorporada > Inhabilitar > Aceptar.

4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

## Acerca de esta tarea

El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Procedimiento

1. Inicie la versión local del asistente.
  - Sistemas operativos AIX Abra el programa dsmsicfgx en el directorio /opt/tivoli/tsm/server/bin. Este asistente sólo puede ejecutarse como usuario root.
  - Sistemas operativos Windows Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Planificación de hojas de trabajo al configurar el sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.

Sistemas operativos AIX Sistemas operativos Linux En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.

Sistemas operativos Windows Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

## Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

## Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

## Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

## Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo dsmserv.opt.
2. Revise los valores de la tabla siguiente y verifique los valores de opciones de servidor, en base al tamaño del sistema.

| Opción de servidor | Valor                                                             |
|--------------------|-------------------------------------------------------------------|
| ACTIVELOGDIRECTORY | Vía de acceso de directorio especificada durante la configuración |
| ACTIVELOGSIZE      | 131072                                                            |
| ARCHLOGCOMPRESS    | No                                                                |
| ARCHLOGDIRECTORY   | Vía de acceso de directorio especificada durante la configuración |
| COMMMETHOD         | TCPIP                                                             |
| COMMTIMEOUT        | 3600                                                              |
| DEVCONFIG          | devconf.dat                                                       |
| EXPINTERVAL        | 0                                                                 |
| IDLETIMEOUT        | 60                                                                |
| MAXSESSIONS        | 500                                                               |

| Opción de servidor | Valor       |
|--------------------|-------------|
| NUMOPENVOLSALLOWED | 20          |
| TCPADMINPORT       | 1500        |
| TCPPORT            | 1500        |
| VOLUMEHISTORY      | volhist.dat |

Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo dsmserv.opt y utilice el mandato SETOPT desde la interfaz de línea de mandatos de administración para establecer las opciones.

Por ejemplo, para actualizar la opción IDLETIMEOUT a 60, emita el siguiente mandato:

```
setopt idletimeout 60
```

3. Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

| Opción de servidor  | Todos los tamaños del sistema                                                                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSLDISABLELEGACYTLS | YES                                                                                                                                                                     |
| SSLFIPSMODE         | NO                                                                                                                                                                      |
| SSLTCPPORT          | Especifique el número de puerto SSL. La unidad de comunicación TCP/IP del servidor espera solicitudes en este puerto para sesiones con SSL activada del cliente.        |
| SSLTCPADMINPORT     | Especifique la dirección del puerto en la que el servidor esperará las solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos. |
| SSLTLS12            | YES                                                                                                                                                                     |

Si alguno de los valores de opción debe actualizarse, edite el archivo dsmserv.opt utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guarde los cambios y cierre el archivo. Si edita el archivo dsmserv.opt directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

## Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

### Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

### Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

## Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

| Característica                            | Más información                                                                                                                                                                                                                                                   |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Distinción entre mayúsculas y minúsculas  | No distingue entre mayúsculas y minúsculas.                                                                                                                                                                                                                       |
| Caducidad de la contraseña predeterminada | 90 días.<br><br>El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor. |
| Intentos de contraseña no válidos         | Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.                                                                                        |
| Longitud de la contraseña                 | El administrador puede especificar una longitud mínima.                                                                                                                                                                                                           |

## Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

| Entidad          | Mandato                                                                               |
|------------------|---------------------------------------------------------------------------------------|
| Nodos de cliente | <ul style="list-style-type: none"><li>• REGISTER NODE</li><li>• UPDATE NODE</li></ul> |

| Entidad         | Mandato                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------|
| Administradores | <ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul> |
| Servidores      | <ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul> |

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:


Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

- Configuración de comunicaciones seguras con Seguridad de la capa de transporte  
Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

#### Tareas relacionadas:

 Protección de las comunicaciones

## Configuración de Centro de operaciones

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

### Antes de empezar

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

### Procedimiento

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

```
https://hostname:secure_port/oc
```

donde:

- *nombre\_host* representa el nombre del sistema donde está instalado Centro de operaciones
- *puerto\_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

Por ejemplo, si el nombre de host es tsm.storage.mylocation.com y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

```
https://tsm.storage.mylocation.com:11090/oc
```

Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.



2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor concentrador configurando el protocolo de la capa de sockets seguros (SSL).

Siga las instrucciones que encontrará en Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

Siga las instrucciones que encontrará en Seguimiento del estado del sistema mediante informes de correo electrónico.

- Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador  
Para proteger las comunicaciones entre Centro de operaciones y el servidor concentrador, añada el certificado de seguridad de la capa de transporte (TLS) del servidor concentrador al archivo de almacén de confianza de Centro de operaciones.

## Registro de la licencia de producto

---

Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.

### Acerca de esta tarea


---

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

### Procedimiento

---

Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.


1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración  y pulsando Creador de mandatos.
3. Emita el mandato REGISTER LICENSE. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

### Qué hacer a continuación

---

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor se ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
-  Sistemas operativos LinuxSi cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

## Definición de las reglas de retención de datos para su empresa

---

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

### Procedimiento

---

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.
3. Pulse el conmutador Configurar y realice los cambios siguientes:
  - Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedores de directorio.
  - Cambie el valor de la columna de copias de seguridad a Sin límite.

- Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador Configurar para que el conjunto de políticas ya no se pueda editar.
  5. Activar el conjunto de políticas pulsando Activar.

## Definición de planificaciones para actividades de mantenimiento del servidor

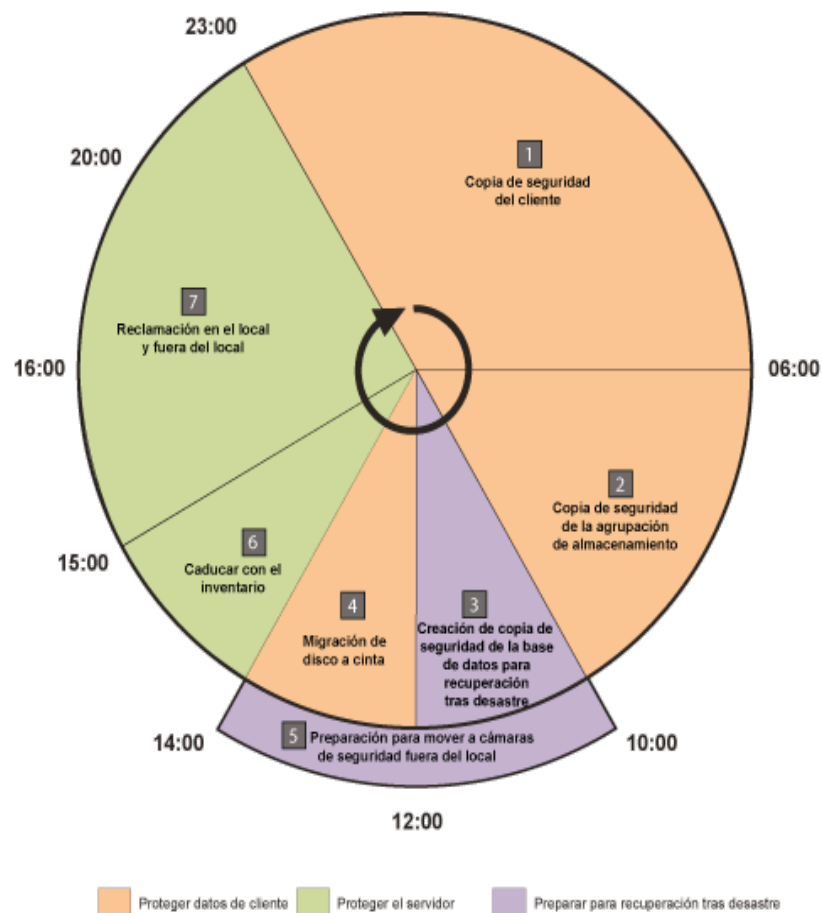
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.

### Acerca de esta tarea

Planifique operaciones de mantenimiento de servidor para ejecutar después de operaciones de copia de seguridad de cliente. Puede controlar la temporización de planificaciones estableciendo la hora de inicio en combinación con la duración para cada operación.

La siguiente figura proporciona un ejemplo de cómo planificar operaciones de mantenimiento.

Figura 1. Planificación diaria de operaciones de servidor para una solución de cinta



La tabla siguiente muestra cómo puede planificar procesos de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de cinta.

| Operación                      | Planificación          |
|--------------------------------|------------------------|
| Copia de seguridad del cliente | Se inicia a las 11 PM. |

| Operación                                                                           | Planificación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Copia de seguridad de agrupaciones de almacenamiento                                | Se inicia a las 6 AM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Proceso para archivos de recuperación tras desastre y de base de datos              | <ul style="list-style-type: none"> <li>La operación de copia de seguridad de base de datos se inicia a las 10 AM, u 11 después de iniciar la operación de copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.</li> <li>La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 5PM o 7 horas después del inicio de la copia de seguridad de la base de datos.</li> <li>La supresión del historial de volumen comienza a las 8 PM, o 10 horas después del inicio de la operación de copia de seguridad de la base de datos.</li> </ul> |
| Preparación de archivos para almacenamiento en cámaras de seguridad fuera del local | Se inicia a las 10 AM, a la misma hora que el procesamiento de los archivos de recuperación tras desastre y base de datos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Migración de disco a cinta                                                          | Se inicia a las 12 PM, o 2 horas después del inicio de la operación de copia de seguridad de la base de datos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Caducidad de inventario                                                             | Se inicia a las 2 PM, o 15 horas después del comienzo de la operación de copia de seguridad del cliente. Este proceso se ejecuta hasta completarse.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reclamación de espacio                                                              | Se inicia a las 3 PM, o 16 horas después del comienzo de la operación de copia de seguridad del cliente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Procedimiento

Tras configurar la clase de dispositivo para las operaciones de copia de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato DEFINE SCHEDULE. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.

- Defina una clase de dispositivo para la operación de seguridad antes de crear la planificación para copias de seguridad de base de datos. Utilice el mandato DEFINE DEVCLASS para crear una clase de dispositivo que se denomine LTOTAPE:

```
define devclass ltotape devtype=lto library=ltolib
```

- Establezca la clase de dispositivo para copias de seguridad de base de datos automáticas. Utilice el mandato SET DBRECOVERY para especificar la clase de dispositivo que ha creado para la copia de seguridad de base de datos en el paso anterior. Por ejemplo, si la clase de dispositivo es LTOTAPE, emita el mandato siguiente:

```
set dbrecovery ltotape
```

- Cree planificaciones para las operaciones de mantenimiento utilizando el mandato DEFINE SCHEDULE. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.

| Operación                                                            | Mandatos de ejemplo e información adicional                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Realice la copia de seguridad de las agrupaciones de almacenamiento. | <p>Cree una planificación para ejecutar el mandato BACKUP STGPOOL. Por ejemplo, emita el siguiente mandato para crear una planificación de copia de seguridad para una agrupación de almacenamiento primario denominada PRIMARY_POOL. La copia de seguridad de la agrupación se realizará en una agrupación de almacenamiento de copias, COPYSTG:</p> <pre>define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1</pre> |
| Realizar una copia de seguridad de la base de datos.                 | <p>Cree una planificación para ejecutar el mandato BACKUP DB. Por ejemplo, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=10:00:00 duration=45 durunits=minutes</pre>                                                     |

| Operación                                                                                 | Mandatos de ejemplo e información adicional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Replique los nodos.</p>                                                                | <p>Opcionalmente, utilice la réplica de nodo para proteger los datos del cliente realizando una copia de seguridad de los datos a un servidor secundario. Para obtener instrucciones, consulte Réplica de datos de cliente en otro servidor. Asegúrese de completar la réplica de nodo antes de iniciar las operaciones de migración.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>Migre los datos de disco a cinta a diario.</p>                                         | <p>Cree una planificación para la migración de agrupación de almacenamiento.</p> <p>Por ejemplo, si una agrupación de almacenamiento de disco se denomina DISKPOOL y la siguiente agrupación de almacenamiento es TAPEPOOL, puede planificar la migración de agrupación de almacenamiento emitiendo el siguiente mandato:</p> <pre>define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days</pre> <p>Para maximizar el rendimiento, puede especificar el número de procesos paralelos que se utilizarán para migrar archivos llevando a cabo los pasos siguientes:</p> <ol style="list-style-type: none"> <li>Para la agrupación de almacenamiento de cinta, asegúrese de que la función de proximidad esté habilitada. Para verificar que la función de proximidad esté habilitada, ejecute el mandato QUERY STGPOOL. Compruebe que se especifica un valor de GROUP, NODE o FILESPACE en el campo COLLOCATE. Si no se especifica un valor de GROUP, NODE o FILESPACE, utilice el mandato UPDATE STGPOOL para especificar COLLOCATE=GROUP, COLLOCATE=NODE o COLLOCATE=FILESPACE, en función de la configuración del sistema.</li> <li>Para la agrupación de almacenamiento de disco, utilice el mandato DEFINE STGPOOL o UPDATE STGPOOL para especificar un valor para el parámetro MIGPROCESS. Por ejemplo, si tiene 12 unidades de cinta, especifique MIGPROCESS=10. De este modo, se utilizan un máximo de 10 unidades de cinta para los procesos de migración. Dos unidades están reservadas para otras tareas, como restauración, copia de seguridad de base de datos y operaciones de copia de seguridad de cliente.</li> </ol> |
| <p>Prepares archivos para almacenamiento en cámaras de seguridad fuera del local.</p>     | <ol style="list-style-type: none"> <li>Mueva los volúmenes de cinta fuera del local siguiendo las instrucciones de Mover soportes de copia de seguridad.</li> <li>Cree el archivo del plan de recuperación tras desastre emitiendo el mandato PREPARE en el servidor de origen: <pre>preparar</pre> </li> <li>Asegúrese de que todos los volúmenes que son necesarios para la recuperación tras desastre se incluyan en el archivo del plan de recuperación. Para obtener más información, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>Realice una copia de seguridad de la información de configuración del dispositivo.</p> | <p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig   filenames=devconfig.dat" active=yes desc="Backup the device   configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Operación                                                                                        | Mandatos de ejemplo e información adicional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Haga una copia de seguridad del historial de volumen.                                            | <p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory   filenames=volhist.dat" active=yes desc="Back up the volume   history." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias. | <p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory   type=dbb todate=today-6 totime=now" active=yes desc="Remove   old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Elimine objetos que exceden su retención permitida.                                              | <p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY.</p> <p>Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar.</p> <p>Por ejemplo, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory   wait=yes resource=8 duration=120" active=yes desc="Remove expired   objects." startdate=today starttime=14:00:00 duration=1 durunits=hours</pre>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Reclame espacio.                                                                                 | <p>Cree una planificación para ejecutar el mandato RECLAIM STGPOOL.</p> <p>Por ejemplo, emita el siguiente mandato para crear una planificación que se denomine RECLAIM:</p> <pre>define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours</pre> <p>Consejo: Para maximizar el rendimiento, puede especificar el número de procesos paralelos que se utilizarán para reclamar espacio. Actualice la agrupación de almacenamiento en cinta utilizando el mandato UPDATE STGPOOL y especifique un valor para el parámetro RECLAIMPROCESS. Por ejemplo, si tiene 12 unidades de cinta, especifique RECLAIMPROCESS=5. Puesto que se utilizan dos unidades para cada proceso de reclamación, el número total de unidades que se pueden utilizar para la reclamación es 10. Dos unidades se reservan para las operaciones de copia de seguridad.</p> |

## Qué hacer a continuación

Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Servidores.
2. Pulse Mantenimiento.

- Mover soportes de copia de seguridad

Para recuperarse de un desastre, necesita volúmenes de copia de seguridad de base de datos, volúmenes de agrupación de almacenamiento de copias y archivos adicionales. Para estar preparado ante un desastre, debe completar tareas diarias.

### Referencia relacionada:

- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)
- DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

### Información relacionada:

- DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Definición de planificaciones de cliente

---

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

### Procedimiento

---

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de Clientes.
2. Pulse Planificaciones.
3. Pulse +Planificación.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.

## Conexión de dispositivos de cinta para el servidor

---

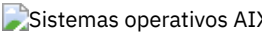
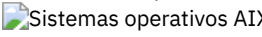
Para que el servidor pueda utilizar un dispositivo de cinta, debe conectar el dispositivo al sistema servidor e instalar el controlador de dispositivo de cinta adecuado

### Acerca de esta tarea

---

Para optimizar el rendimiento del sistema, utilice dispositivos de cinta rápidos y de gran capacidad. Suministre suficientes unidades de cinta para cumplir los requisitos empresariales.

Conecte los dispositivos de cinta a su propio adaptador de bus de host (HBA), no compartidos con otros tipos de dispositivos tales como discos.. Las unidades de cinta de IBM® tienen ciertos requisitos especiales en cuanto a los HBA y los controladores asociados.

-  Sistemas operativos AIX/Sistemas operativos Linux Conectar un dispositivo de biblioteca automática a su dispositivo  
Puede conectar un dispositivo de biblioteca automatizada a su sistema para almacenar datos en cinta.
- Seleccionar un controlador de dispositivo de cinta  
Para utilizar dispositivos de cinta con IBM Spectrum Protect debe instalar el controlador de dispositivo de cinta adecuado.
-  Sistemas operativos AIX/Sistemas operativos Linux Nombres de archivo especiales para dispositivos de cinta  
Se requiere un nombre de archivo especial para que el servidor de IBM Spectrum Protect pueda operar con dispositivos de cinta, de cambiador de medios o de medios extraíbles.
- Instalación y configuración de controladores de dispositivos de cinta  
Para poder utilizar dispositivos de cinta con IBM Spectrum Protect, debe instalar el controlador de dispositivo de cinta correcto.

## Conectar un dispositivo de biblioteca automática a su dispositivo

---

Puede conectar un dispositivo de biblioteca automatizada a su sistema para almacenar datos en cinta.

### Acerca de esta tarea

---

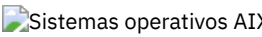
Antes de adjuntar un dispositivo de biblioteca automatizada, tenga en cuenta las siguientes restricciones:

- Los dispositivos conectados deben estar en su propio adaptador de bus de host (HBA).
- Un HBA no se puede compartir con otros tipos de dispositivo como por ejemplo un disco..
- En el caso de HBA de canal de fibra multipuerto, los dispositivos deben estar conectados en su puerto propio. Estos puertos no se pueden compartir con otros tipos de dispositivo.
- Las unidades de cinta de IBM® tienen ciertos requisitos especiales en cuanto a HBA y los controladores asociados. Para obtener más información acerca de los dispositivos, consulte el sitio web sobre su sistema operativo :
  - Dispositivos soportados de IBM Spectrum Protect para AIX
  - Dispositivos soportados de IBM Spectrum Protect para Linux y Windows

### Procedimiento

---

Para utilizar el adaptador de canal de fibra (FC), siga estos pasos:

1. Instale el adaptador FC y los controladores asociados.
  2. Instale los controladores de dispositivo pertinentes para los dispositivos del cambiador de medios.
-  Sistemas operativos AIX/Sistemas operativos Linux Configuración de la modalidad de biblioteca  
Para que el servidor de IBM Spectrum Protect acceda a una biblioteca SCSI, el dispositivo de cinta debe estar en la modalidad adecuada.

**Conceptos relacionados:**

Seleccionar un controlador de dispositivo de cinta

## Seleccionar un controlador de dispositivo de cinta

---

Para utilizar dispositivos de cinta con IBM Spectrum Protect debe instalar el controlador de dispositivo de cinta adecuado.

- Controladores de dispositivos de cinta de IBM  
Hay controladores de dispositivos de cinta IBM® disponibles para la mayoría de dispositivos de cinta etiquetados de IBM.
- Controladores de dispositivos de cinta de IBM Spectrum Protect  
El servidor de IBM Spectrum Protect proporciona controladores de dispositivos de cinta.

**Referencia relacionada:**

Instalación y configuración de controladores de dispositivos de cinta

## Controladores de dispositivos de cinta de IBM

---

Hay controladores de dispositivos de cinta IBM® disponibles para la mayoría de dispositivos de cinta etiquetados de IBM.

Puede descargar controladores de dispositivos de cinta de IBM en el sitio web de Fix Central:

1. Vaya al sitio web de Fix Central: Sitio web de Fix Central.
2. Pulse en Seleccionar producto.
3. Seleccione Sistemas de almacenamiento en el menú Grupo de productos.
4. Seleccione Sistemas de cintas en el menú Almacenamiento del sistema.
5. Seleccione Controladores y software para dispositivos de cinta en el menú Sistemas de cintas.
6. Seleccione Controladores de dispositivo de cinta en el menú Controladores y software para cintas. Además de las unidades de cinta, también tiene acceso a herramientas tales como la IBM Tape Diagnostic Tool (ITDT).
7. Seleccione el sistema operativo en el menú Plataforma.

 Sistemas operativos AIX  Sistemas operativos Windows

Para obtener la lista más actualizada de dispositivos y niveles de sistema operativo soportados por los controladores de dispositivos de cinta de IBM, consulte el sitio web Dispositivos soportados por IBM Spectrum Protect en Dispositivos soportados para AIX y Windows.

 Sistemas operativos Linux

Para obtener la lista más actualizada de dispositivos de cinta y niveles de sistema operativo soportados por los controladores de dispositivos de cinta de IBM, consulte el sitio web Dispositivos soportados por IBM Spectrum Protect en Dispositivos soportados para Linux.


Los controladores de dispositivos de cinta de IBM solo admiten algunos niveles de kernel de Linux. Para obtener información sobre los niveles de kernel soportados, consulte Sitio web de Fix Central.

## Controladores de dispositivos de cinta de IBM Spectrum Protect

---

El servidor de IBM Spectrum Protect proporciona controladores de dispositivos de cinta.

Un controlador de dispositivo de cinta de IBM Spectrum Protect se instala junto con el servidor

 Sistemas operativos AIX

Puede utilizar el controlador de dispositivos de cinta SCSI genérico que proporciona el sistema operativo IBM® AIX para trabajar con dispositivos de cinta que no estén soportados por el controlador de dispositivos IBM Spectrum Protect. Si se utiliza controlador de dispositivo de cinta SCSI genérico de AIX, la clase de dispositivo GENERICTAPE se debe establecer en el tipo de dispositivo que se haya especificado en el mandato DEFINE DEVCLASS.

Para los siguientes dispositivos de cinta, puede elegir si desea instalar el controlador de dispositivo de cinta de IBM Spectrum Protect o el controlador de dispositivo nativo de su sistema operativo:

- ECART
- LTO (no de IBM)

Todas las bibliotecas conectadas a SCSI que contienen unidades de cinta de la lista deben utilizar el controlador del conmutador de IBM Spectrum Protect.

Los controladores de dispositivo de cinta adquiridos de otros proveedores de hardware se pueden utilizar si se asocian a la clase de dispositivo GENERICTAPE. Los controladores de dispositivo genéricos no están admitidos en las clases de dispositivo WORM (write-one read-many).

#### Sistemas operativos Linux


Puede utilizar el controlador de dispositivo Passthru IBM Spectrum Protect. Los controladores de dispositivo passthru IBM Spectrum Protect requieren que el controlador de dispositivo de Linux genérico de SCSI (sg) junto con el sistema operativo Linux instalen los kernels.

Por ejemplo, puede instalar el controlador de dispositivo Passthru IBM Spectrum Protect para los siguientes dispositivos de cinta:

- ECART
- LTO (no de IBM)

Todas las bibliotecas conectadas a SCSI que contengan unidades de cinta que no estén etiquetadas por IBM en la lista también deben utilizar el controlador de dispositivos Passthru de IBM Spectrum Protect.

No puede utilizar el controlador de dispositivo (st) de cinta SCSI genérico que proporciona el sistema operativo Linux. Así pues, el tipo de dispositivo GENERICTAPE no está soportado para el mandato DEFINE DEVCLASS.

 Sistemas operativos Windows Puede seleccionar un controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab en lugar del controlador de dispositivo de IBM Spectrum Protect. El controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab solo se puede utilizar para dispositivos que tengan una etiqueta que no sea IBM y para unidades de cinta que no sean IBM. Para el controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab, puede seleccionar el controlador de dispositivo passthru de SCSI IBM Spectrum Protect o el controlador de dispositivo de cinta nativo de Windows. Si se utiliza el controlador de dispositivo passthru SCSI, la clase de dispositivo definida en el mandato DEFINE DEVCLASS no puede ser GENERICTAPE. Si se utiliza el controlador de dispositivo nativo, la clase de dispositivo debe ser GENERICTAPE.

## Nombres de archivo especiales para dispositivos de cinta

Se requiere un nombre de archivo especial para que el servidor de IBM Spectrum Protect pueda operar con dispositivos de cinta, de cambiador de medios o de medios extraíbles.

#### Sistemas operativos AIX

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 1 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a la unidad o biblioteca. Puede utilizar el mandato de sistema operativo SMIT para obtener el nombre de archivo especial de dispositivo. En los ejemplos, x especifica un entero, 0 o mayor.

Tabla 1. Ejemplos de dispositivo

| Dispositivo                                                                                         | Ejemplo de dispositivo | Nombre de archivo lógico |
|-----------------------------------------------------------------------------------------------------|------------------------|--------------------------|
| Unidades de cinta que puede utilizar el controlador de dispositivo de IBM Spectrum Protect          | /dev/mtx               | mtx                      |
| Unidades de cinta que puede utilizar el controlador de dispositivo de cinta de IBM                  | /dev/rmtx              | rmtx                     |
| Unidades de cinta que puede utilizar el controlador de dispositivo de cinta genérico de IBM AIX     | /dev/mtx               | rmtx                     |
| Dispositivos de biblioteca que puede utilizar el controlador de dispositivo de IBM Spectrum Protect | /dev/lbx               | lbx                      |
| Dispositivos de biblioteca que puede utilizar el controlador de dispositivo de cinta de IBM         | /dev/smcx              | smcx                     |

#### Sistemas operativos Linux

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 2 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a una unidad o biblioteca. En los ejemplos, x especifica un entero, 0 o mayor.

Tabla 2. Ejemplos de dispositivo

| Dispositivo                                                                                         | Ejemplo de dispositivo | Nombre de archivo lógico |
|-----------------------------------------------------------------------------------------------------|------------------------|--------------------------|
| Unidades de cinta que puede utilizar el controlador de dispositivo passthru de IBM Spectrum Protect | /dev/tmsmcsi/mtx       | mtx                      |
| Unidades de cinta que puede utilizar el controlador de dispositivo lin_tape de IBM                  | /dev/IBMtapex          | IBMtapex                 |



| Dispositivo                                                                                                  | Ejemplo de dispositivo | Nombre de archivo lógico |
|--------------------------------------------------------------------------------------------------------------|------------------------|--------------------------|
| Dispositivos de biblioteca que puede utilizar el controlador de dispositivo passthru de IBM Spectrum Protect | /dev/tmscsi/lbx        | lbx                      |
| Dispositivos de biblioteca que puede utilizar el controlador de dispositivo lin_tape de IBM                  | /dev/IBMchangerx       | IBMchangerx              |

#### Sistemas operativos Windows

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 3 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a una unidad o biblioteca. En los ejemplos, *a*, *b*, *c*, *d* y *x* especifican un entero, 0 o mayor, donde:

- *a* especifica el ID de destino.
- *b* especifica el LUN.
- *c* especifica el ID de bus SCSI.
- *d* especifica el ID de puerto.




Tabla 3. Ejemplos de dispositivo

| Dispositivo                                                                                             | Ejemplo de dispositivo | Nombre dispositivo convertido |
|---------------------------------------------------------------------------------------------------------|------------------------|-------------------------------|
| Unidades de cinta admitidas por el controlador de dispositivo de IBM Spectrum Protect                   | <i>mta.b.c.d</i>       | <i>mta.b.c.d</i>              |
| Unidades de cinta admitidas por el controlador de dispositivo passthru de IBM Spectrum Protect          | <i>mta.b.c.d</i>       | <i>mta.b.c.d</i>              |
| Unidades de cinta admitidas por el controlador de dispositivo de IBM                                    | Tapex                  | <i>mta.b.c.d</i>              |
| Dispositivos de biblioteca admitidos por el controlador de dispositivo de IBM Spectrum Protect          | <i>lb.a.b.c.d</i>      | <i>lba.b.c.d</i>              |
| Dispositivos de biblioteca admitidos por el controlador de dispositivo passthru de IBM Spectrum Protect | <i>lba.b.c.d</i>       | <i>lba.b.c.d</i>              |
| Dispositivos de biblioteca admitidos por el controlador de dispositivo de IBM                           | Changerx               | <i>lba.b.c.d</i>              |

## Instalación y configuración de controladores de dispositivos de cinta

Para poder utilizar dispositivos de cinta con IBM Spectrum Protect, debe instalar el controlador de dispositivo de cinta correcto.

IBM Spectrum Protect admite todos los dispositivos que están soportados por los controladores de dispositivos de cinta de IBM®. No obstante, IBM Spectrum Protect no admite todos los niveles de sistema operativo que admiten los controladores de dispositivos de cinta de IBM.


- **Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM**  
Instale y configure un controlador de dispositivo de cinta de IBM para utilizar un dispositivo de cinta de IBM SCSI
-  **Sistemas operativos AIX** Configuración de controladores de dispositivos de cinta en sistemas AIX  
Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta no IBM en sistemas AIX.
-  **Sistemas operativos Linux** Configuración de controladores de dispositivos de cinta en sistemas Linux  
Consulte los temas siguientes al instalar y configurar los controladores de dispositivos de cinta en sistemas Linux.
-  **Sistemas operativos Windows** Configuración de controladores de dispositivos de cinta en sistemas Windows  
Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta y bibliotecas en sistemas Windows.

## Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM

Instale y configure un controlador de dispositivo de cinta de IBM® para utilizar un dispositivo de cinta de IBM SCSI

### Acerca de esta tarea

Para obtener instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*.

 **Sistemas operativos AIX** Después de completar el procedimiento de instalación en la publicación *IBM Tape Device Drivers Installation and User's Guide*, se emiten mensajes diferentes, dependiendo del controlador de dispositivo que desee instalar. Si está instalando el controlador de dispositivo para una unidad de cinta o de biblioteca de IBM se devolverán los mensajes siguientes:

```
rmtx disponible
```

```
o
```

```
smcx disponible
```


Tome nota del valor de x, que asigna el controlador de dispositivo de cinta de IBM. Para determinar el nombre de archivo especial del dispositivo, emita uno de los siguientes mandatos:

- Para unidades de cinta, `ls -l /dev/rmt*`
- Para bibliotecas de cintas, `ls -l /dev/smc*`

Es posible que el nombre de archivo tenga más caracteres al final para indicar características operativas diferentes, pero IBM Spectrum Protect no necesita estos caracteres. Para los controladores de dispositivo de IBM utilice el nombre del archivo base en el parámetro DEVICE del mandato DEFINE PATH para asignar un dispositivo a una unidad (/dev/rmtx) o a una biblioteca (/dev/smcx).

Después de instalar el controlador de dispositivo, puede utilizar la herramienta System Management Interface Tool (SMIT) para configurar unidades de cinta y bibliotecas de cintas no IBM. Realice los pasos siguientes:

1. Ejecute el programa SMIT.
2. Pulse en Dispositivos.
3. Pulse Dispositivos de IBM Spectrum Protect.
4. Pulse Dispositivos conectados a la SAN de canal de fibra.
5. Pulse Descubrir dispositivos soportados por IBM Spectrum Protect. Espere a que se complete el proceso de descubrimiento.
6. Vuelva al menú de Dispositivos conectados a la SAN de canal de fibra y pulse Listar atributos de un dispositivo detectado.

 **Sistemas operativos Linux** Después de completar el procedimiento de instalación en la publicación *IBM Tape Device Drivers Installation and User's Guide*, se emiten mensajes diferentes, dependiendo del controlador de dispositivo que desee instalar. Si está instalando el controlador de dispositivo para un dispositivo IBM LTO o 3592, se devuelven los siguientes mensajes:

```
IBMtapex disponible
```

```
o
```


```
IBMChangerx disponible
```

Tome nota del valor de x, que asigna el controlador de dispositivo de cinta de IBM. Para determinar el nombre de archivo especial del dispositivo, emita uno de los siguientes mandatos:

- Para unidades de cinta, `ls -l /dev/IBMtape*`
- Para bibliotecas de cintas, `ls -l /dev/IBMChange*`

Es posible que el nombre de archivo tenga más caracteres al final para indicar características operativas diferentes, pero IBM Spectrum Protect no necesita estos caracteres. Para controladores de dispositivo IBM, utilice el nombre de archivo base en el parámetro DEVICE del mandato DEFINE PATH para asignar un dispositivo a una unidad (/dev/IBMtapex) o a una biblioteca (/dev/IBMChangerx).

Restricción: El tipo de dispositivo de esta clase no debe ser GENERICTAPE.

 **Sistemas operativos Windows** Para sistemas operativos Windows, IBM Spectrum Protect proporciona dos controladores de dispositivo.

**Controlador de dispositivo Passthru**

Si el fabricante del dispositivo de cinta proporciona un controlador de dispositivo SCSI, instale el controlador de dispositivo passthru IBM Spectrum Protect passthru



**Controlador de dispositivo SCSI para dispositivos de cinta**

Si el fabricante del dispositivo de cinta no proporciona un controlador de dispositivo SCSI, instale el controlador de dispositivo SCSI IBM Spectrum Protect para dispositivos de cinta. El nombre del archivo de controlador es tsm SCSI64.sys.

Para instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*. Después de instalar el controlador de dispositivo de cinta de IBM, el servidor especifica un nombre de archivo especial, TapeX, para las unidades de cinta de IBM, o ChangerY, para los conmutadores de soporte de IBM. Para un controlador de dispositivo SCSI IBM Spectrum Protect o un controlador de dispositivo passthru IBM Spectrum Protect, puede emitir un mandato del sistema operativo Windows, regedit, para verificar el nombre de archivo del archivo especial y el controlador. El servidor IBM Spectrum Protect también proporciona un programa de utilidad para comprobar el dispositivo en el sistema operativo Windows. El programa de utilidad, tsm dlist, se incluye en el paquete de servidor. Para utilizar el programa de utilidad, complete los siguientes pasos:


1. Asegúrese de que la interfaz de programación de aplicaciones (API) del adaptador de bus de host esté instalado
2. Para obtener información de dispositivo del sistema host, escriba:

tsmdlst

-  Sistemas operativos AIX  Sistemas operativos Linux Acceso de entrada/salida con dispositivos de cinta IBM La entrada/salida multivía de acceso es una técnica que utiliza distintas vías de acceso para acceder al mismo dispositivo físico, por ejemplo mediante varios adaptadores de bus de host (HBA) o conmutadores. El uso de la técnica multivía de acceso ayuda a asegurarse de que no se produzca un único punto de anomalía.

#### Conceptos relacionados:

Acceso de entrada/salida con dispositivos de cinta IBM

 Sistemas operativos AIX

## Configuración de controladores de dispositivos de cinta en sistemas AIX





---


Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta no IBM® en sistemas AIX.

### Acerca de esta tarea

---

Para obtener instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*.

-  Sistemas operativos AIX Dispositivos SCSI y de canal de fibra Las solicitudes y los menús de definición de dispositivos de IBM Spectrum Protect en SMIT permiten gestionar los dispositivos SCSI y FC (canal de fibra) conectados.
-  Sistemas operativos AIX Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autocambiadores de bibliotecas que no son IBM.
-  Sistemas operativos AIX Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autoconmutadores de bibliotecas adquiridas al proveedor.
-  Sistemas operativos AIX Configuración de dispositivos conectados a SAN de canal de fibra Para configurar un dispositivo conectado a SAN de canal de fibra, complete este procedimiento.

 Sistemas operativos AIX

## Dispositivos SCSI y de canal de fibra

---

Las solicitudes y los menús de definición de dispositivos de IBM Spectrum Protect en SMIT permiten gestionar los dispositivos SCSI y FC (canal de fibra) conectados.

El menú principal de IBM Spectrum Protect tiene dos opciones:

Dispositivos SCSI conectados

Utilice esta opción para configurar dispositivos SCSI que estén conectados a un adaptador SCSI en el host.

Dispositivos conectados de red de área de almacenamiento (SAN) de canal de fibra

Utilice esta opción para configurar dispositivos que estén conectados a un adaptador FC en el host. Seleccione uno de los siguientes atributos:

Lista atributos de un dispositivo descubierto

Lista atributos de un dispositivo conocido en la base de datos ODM actual.

- ID de puerto FC:

Es el ID de puerto FC de 24 bits ID(N(L)\_Puerto o F(L)\_Puerto). Es el identificador de dirección exclusivo en la topología asociada a la que está conectado el dispositivo. En los entornos de conmutador o de tejido, generalmente viene determinado por el conmutador, con los 2 bytes superiores que no sean cero. En un bucle arbitrado privado, es la dirección física del bucle arbitrado (AL\_PA), en la que los 2 bytes superiores tienen el valor cero. Póngase en contacto con los proveedores de FC para saber cómo se asigna una dirección AL\_PA o un ID de puerto.

- ID de LUN correlacionado:

Un sistema de puente de FC a SCSI (denominado también convertidor, direccionador o pasarela). Póngase en contacto con los proveedores de puentes para saber cómo deben correlacionarse los LUN. Es recomendable no cambiar los ID de los LUN correlacionados.

- Nombre WW:

Nombre de ámbito mundial (WWN) del puerto al que está conectado el dispositivo. Es el identificador exclusivo de 64 bits que asignan los proveedores de componentes FC, tales como puentes o dispositivos FC nativos. Póngase en contacto con los proveedores de FC para saber cuál es el valor de WWN de un puerto.

- ID de producto:

ID de producto del dispositivo. Póngase en contacto con los proveedores de los dispositivos para determinar el ID de producto.

#### Detectar dispositivos soportados por IBM Spectrum Protect


Mediante esta opción se descubren los dispositivos de una red SAN FC admitidos por IBM Spectrum Protect y dichos dispositivos pasan a estar disponibles. Si agrega o elimina un dispositivo de un entorno SAN existente, deberá detectar de nuevo los dispositivos mediante esta opción. En primer lugar deben detectarse los dispositivos, de modo que los valores actuales de los atributos de los dispositivos aparezcan en la opción Listar atributos de un dispositivo detectado. Los dispositivos admitidos en redes SAN FC son unidades de cinta, autocambiadores. El controlador de dispositivo de IBM Spectrum Protect pasa por alto todos los tipos de dispositivo, como por ejemplo, un disco.

#### Eliminar todos los dispositivos definidos

Mediante esta opción se eliminan todos los dispositivos de IBM Spectrum Protect conectados a la red SAN FC cuyo estado está establecido en `DEFINED` en la base de datos de ODM. En caso necesario, detecte de nuevo los dispositivos mediante la opción `Detectar dispositivos soportados por IBM Spectrum Protect` una vez que haya eliminado todos los dispositivos definidos.

#### Eliminar un dispositivo

esta opción elimina un único dispositivo de IBM Spectrum Protect conectado a la red SAN FC cuyo estado es `DEFINED` en la base de datos ODM. En caso necesario, detecte de nuevo el dispositivo mediante la opción `Detectar dispositivos soportados por IBM Spectrum Protect` una vez que haya eliminado un dispositivo definido.

 Sistemas operativos AIX

## Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores

---

Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autocambiadores de bibliotecas que no son IBM.

### Procedimiento


---

Ejecute el programa SMIT para configurar el controlador de dispositivo para cada autocambiador o robot:

1. Seleccione Dispositivos.
2. Seleccione IBM Spectrum ProtectDispositivos.
3. Seleccione Biblioteca/Cambiador de medios.
4. Seleccione Agregar una biblioteca/Cambiador de medios.
5. Seleccione IBM Spectrum Protect-SCSI-LB para cualquier biblioteca admitida por IBM Spectrum Protect.
6. Seleccione el adaptador padre en el que va a conectar el dispositivo. Este número figura con el formato: 00-0X, siendo X la ubicación del número de ranura de la tarjeta adaptadora SCSI.
7. Cuando se le solicite, entre la dirección de conexión (`CONNECTION`) del dispositivo que está instalando. La dirección de conexión es un número de dos dígitos. El primero de ellos es el ID SCSI (el valor que ha anotado en la hoja de trabajo). El segundo es el número de unidad lógica (LUN) SCSI del dispositivo, que suele ser cero a menos que se indique lo contrario. El ID SCSI y el LUN deben estar separados por una coma (,). Por ejemplo, una dirección de conexión de 4,0 tiene un SCSI ID=4 y un LUN=0.
8. Pulse DO.

Recibirá un mensaje (nombre de archivo lógico) con el formato `lbX disponible`. Tome nota del valor de X, que es un número que asigna el sistema de forma automática. Utilice esta información para completar el campo Nombre de dispositivo en la hoja de trabajo.

Por ejemplo, si el mensaje es `lb0 Available`, el campo Nombre de dispositivo es `/dev/lb0` en la hoja de trabajo. Utilice siempre el prefijo `/dev/` con el nombre proporcionado por SMIT.

 Sistemas operativos AIX

## Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta

---

Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autoconmutadores de bibliotecas adquiridas al proveedor.

## Procedimiento

---

Importante: IBM Spectrum Protect no puede sobrescribir cintas *tar* ni *dd*, pero las cintas *tar* o *dd* pueden sobrescribir cintas de IBM Spectrum Protect.


Restricción: las unidades de cinta sólo pueden compartirse cuando no se ha definido la unidad o cuando no se ha iniciado el servidor. El mandato MKSYSB no funciona cuando IBM Spectrum Protect y AIX comparten las mismas unidades. Para utilizar el controlador de dispositivo de cintas nativo del sistema operativo junto con una unidad SCSI, el dispositivo debe configurarse primero para AIX y, a continuación, para IBM Spectrum Protect. Consulte la documentación de AIX relacionada con estos controladores de dispositivo nativos.

Ejecute el programa SMIT para configurar el controlador de dispositivo para cada una de las unidades (incluidas las de la biblioteca) de la forma siguiente:

1. Seleccione Dispositivos.
2. Seleccione IBM Spectrum ProtectDispositivos.
3. Seleccione Unidad de cinta.
4. Seleccione Añadir una unidad de cinta.
5. Seleccione IBM Spectrum Protect-SCSI-MT para cualquier unidad de cinta soportada.
6. Seleccione el adaptador al que va a conectar el dispositivo. Este número figura con el formato: 00-0X, siendo X la ubicación del número de ranura de la tarjeta adaptadora SCSI.
7. Cuando se le solicite, entre la dirección de conexión (CONNECTION) del dispositivo que está instalando. La dirección de conexión es un número de dos dígitos. El primero de ellos es el ID SCSI (el valor que ha anotado en la hoja de trabajo). El segundo es el número de unidad lógica (LUN) SCSI del dispositivo, que suele ser cero a menos que se indique lo contrario. El ID SCSI y el LUN deben estar separados por una coma (,). Por ejemplo, una dirección de conexión de 4,0 tiene un SCSI ID=4 y un LUN=0.
8. Pulse DO. Recibirá un mensaje:

Si está configurando el controlador de dispositivo para un dispositivo de cinta (que no sea IBM®), recibirá un mensaje (nombre de archivo lógico) con el formato `mtX Disponible`. Tome nota del valor de X, que es un número que asigna el sistema de forma automática. Utilice esta información para completar el campo Nombre de dispositivo en la hoja de trabajo.

Por ejemplo, si el mensaje es `mt0 Available`, el campo Nombre de dispositivo es `/dev/mt0` en la hoja de trabajo. Utilice siempre el prefijo `/dev/` con el nombre proporcionado por SMIT.

 Sistemas operativos AIX

## Configuración de dispositivos conectados a SAN de canal de fibra

---

Para configurar un dispositivo conectado a SAN de canal de fibra, complete este procedimiento.

### Procedimiento

---



1. Ejecute el programa SMIT.
2. Seleccione Dispositivos.
3. Seleccione IBM Spectrum ProtectDispositivos.
4. Seleccione Dispositivos conectados a la SAN de canal de fibra.
5. Seleccione Detectar dispositivos soportados por IBM Spectrum Protect. El proceso de detección puede tardar cierto tiempo.
6. Vuelva al menú Canal de fibra y seleccione Listar atributos de un dispositivo detectado.
7. Anote el identificador de dispositivo de tres caracteres, que utiliza al definir una vía de acceso al dispositivo en IBM Spectrum Protect. Por ejemplo, si una unidad de cintas tiene el identificador `mt2`, especifique `/dev/mt2` como el nombre de dispositivo.

 Sistemas operativos Linux



## Configuración de controladores de dispositivos de cinta en sistemas Linux


---

Consulte los temas siguientes al instalar y configurar los controladores de dispositivos de cinta en sistemas Linux.

-  Sistemas operativos Linux Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas  
Para utilizar el controlador de paso a través de IBM Spectrum Protect Linux, debe llevar a cabo los siguientes pasos.
-  Sistemas operativos Linux Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfcp)  
El controlador de dispositivo zfcp (zSeries Linux Fibre Channel Adapter) es un controlador de adaptador especial en el sistema

IBM® zSeries.

-  Sistemas operativos Linux Información sobre los dispositivos SCSI del sistema  
En el archivo `/proc/scsi/scsi` encontrará información acerca de los dispositivos que detecta el sistema. Este archivo contiene una lista de todos los dispositivos SCSI detectados.
-  Sistemas operativos Linux Impedir que las etiquetas de cinta se sobrescriban  
El controlador del dispositivo IBM Spectrum Protect Passthru usa el controlador de dispositivo genérico (sg) de Linux SCSI para controlar y operar dispositivos de cinta que están conectados al sistema. Si el controlador de dispositivos de cinta SCSI genérico (st) de Linux se carga en el kernel y configura los dispositivos de cinta conectados, pueden surgir conflictos sobre cómo se gestiona un dispositivo puesto que tanto el controlador genérico sg como el controlador st controlan el mismo dispositivo.

 Sistemas operativos Linux

## Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas

---

Para utilizar el controlador de paso a través de IBM Spectrum Protect Linux, debe llevar a cabo los siguientes pasos.

### Procedimiento

---

1. Verifique que el dispositivo esté conectado a su sistema, que esté encendido y activo.
2. Verifique si el sistema ha detectado correctamente el dispositivo ejecutando este mandato:

```
cat /proc/scsi/scsi
```

3. Asegúrese de que tanto el paquete de controladores de dispositivo IBM Spectrum Protect (tmsmcsi) como el paquete del servidor de almacenamiento estén instalados.
4. Hay disponibles dos métodos de configuración del controlador en el paquete de controladores del dispositivo de IBM Spectrum Protect: `autoconf` y `tmsmcsi`. Ambos métodos llevan a cabo las tareas siguientes:
  - Carga del controlador genérico (sg) SCSI de Linux en el kernel.
  - Creación de los archivos especiales necesarios para el controlador Passthru.
  - Creación de archivos de información de dispositivo para los dispositivos de cinta (`/dev/tmsmcsi/mtinfo`) y las bibliotecas (`/dev/tmsmcsi/lbinfo`).
5. Ejecute el método de configuración que prefiera (`autoconf` o `tmsmcsi`) para el controlador passthru IBM Spectrum Protect.
  - Para ejecutar el método de configuración `autoconf`, emita el siguiente mandato:

```
autoconf
```

- Para ejecutar el método de configuración `tmsmcsi`, emita el siguiente mandato:
    - a. Copie los dos archivos de configuración de ejemplo que se encuentran en el directorio de instalación desde `mt.conf.smp` y `lb.conf.smp` a `mt.conf` y `lb.conf`, respectivamente.
    - b. Edite los archivos `mt.conf` y `lb.conf`. Agregue una stanza (como se muestra en el ejemplo al inicio del archivo) para cada destino de SCSI, ID y combinación de LUN. Cada combinación de entradas de LUN, ID y destino de SCSI corresponde a una biblioteca o unidad de cintas que desea configurar. Asegúrese de que los archivos cumplen con estos requisitos:
      - Elimine el ejemplo que figura al principio de los archivos.
      - Debe haber una línea nueva entre cada sección.
      - Debe haber una nueva línea después de la última sección.
      - Asegúrese de que no hay signos de almohadilla (#) en ningún archivo.
    - c. Ejecute el script `tmsmcsi` desde el directorio de instalación del controlador de dispositivo.
6. Verifique que el dispositivo está configurado debidamente examinando los archivos de texto correspondientes a los dispositivos de cinta (`/dev/tmsmcsi/mtinfo`) y a las bibliotecas (`/dev/tmsmcsi/lbinfo`).
  7. Determine los nombres de archivos especiales para las unidades de cinta y bibliotecas:
    - Para determinar los nombres de los dispositivos de cinta, ejecute el mandato siguiente:

```
> ls /dev/tmsmcsi/mt*
```

- Para determinar los nombres de las bibliotecas, emita el mandato siguiente:

```
> ls /dev/tmsmcsi/lb*
```

Esta información le ayuda a identificar los nombres de archivos especiales de `/dev/tmsmcsi/mtx` y `/dev/tmsmcsi/lbx` a proporcionar al servidor al emitir un mandato `DEFINE PATH`.

### Qué hacer a continuación

---

Si reinicia el sistema host, debe volver a ejecutar el script autoconf o tsm SCSI para volver a configurar los dispositivos IBM Spectrum Protect. Si reinicia la instancia de servidor IBM Spectrum Protect, no tendrá que volver a configurar los dispositivos. En general, el controlador genérico SCSI de Linux está precargado en el kernel. Para verificar que el controlador se encuentra en el kernel, emita el siguiente mandato:

```
> lsmod | grep sg
```

Si el controlador no está en el kernel, emita el mandato modprobe sg para cargar el controlador sg en el kernel.

 Sistemas operativos Linux

## Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfcp)

El controlador de dispositivo zfcp (zSeries Linux Fibre Channel Adapter) es un controlador de adaptador especial en el sistema IBM® zSeries.

### Acerca de esta tarea

Los controladores de dispositivo de cinta de IBM Spectrum Protect e IBM pueden ejecutarse en las plataformas zSeries con sistemas operativos Linux en entornos de 64 bits, y dan soporte a la mayoría de dispositivos de cinta OEM (original equipment manufacturer) de dispositivos de cinta IBM con interfaces de canal de fibra.

Para obtener más información sobre el controlador zfcp, consulte el Redpaper de IBM, *Getting Started with zSeries Fibre Channel Protocol*, que está disponible en IBM Redbooks.

### Procedimiento

1. Cargue el módulo qdio.
2. Instale el controlador zfcp.
3. Correlacione el protocolo de canal de fibra (FCP) y configure el controlador zfcp.
4. Instale y configure el controlador de dispositivo de cinta de IBM.


 Sistemas operativos Linux

## Información sobre los dispositivos SCSI del sistema

En el archivo `/proc/scsi/scsi` encontrará información acerca de los dispositivos que detecta el sistema. Este archivo contiene una lista de todos los dispositivos SCSI detectados.

Dispone de la información de dispositivos siguiente: el número de host, el número de canal, el ID de SCSI, el número de unidad lógica, el proveedor, el nivel de firmware, el tipo de dispositivo y la modalidad de SCSI. Por ejemplo, si un sistema contiene algunas bibliotecas StorageTek e IBM®, una pasarela de SAN y algunas unidades Quantum DLT, el archivo `/proc/scsi/scsi` tendrá un aspecto similar al siguiente:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
 Vendor: STK Model: 9738 Rev: 2003
 Type: Medium Changer ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
 Vendor: PATHLIGHT Model: SAN Gateway Rev: 32aC
 Type: Unknown ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
 Vendor: QUANTUM Model: DLT7000 Rev: 2560
 Type: Sequential-Access ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
 Vendor: IBM Model: 7337 Rev: 1.63
 Type: Medium Changer ANSI SCSI revision: 02
```

 Sistemas operativos Linux

## Impedir que las etiquetas de cinta se sobrescriban

El controlador del dispositivo IBM Spectrum Protect Passthru usa el controlador de dispositivo genérico (sg) de Linux SCSI para controlar y operar dispositivos de cinta que están conectados al sistema. Si el controlador de dispositivos de cinta SCSI genérico (st) de



Linux se carga en el kernel y configura los dispositivos de cinta conectados, pueden surgir conflictos sobre cómo se gestiona un dispositivo puesto que tanto el controlador genérico sg como el controlador st controlan el mismo dispositivo.

## Acerca de esta tarea

---

Si el controlador st controla dispositivos utilizados por IBM Spectrum Protect, es posible que las etiquetas de cinta internas de IBM Spectrum Protect se sobregaben y se pierdan datos. Si una aplicación utiliza el controlador st para controlar dispositivos y no se especifica la opción non-rewind, las cintas se rebobinan automáticamente tras finalizar una operación. La operación de rebobinado automático reubica la posición del cabezal de cinta al principio de la cinta. Si la cinta permanece cargada en la unidad, la siguiente operación de grabación que no sea de IBM Spectrum Protect sobrescribirá la etiqueta de la cinta de IBM Spectrum Protect porque la etiqueta está al principio de la cinta.

Para impedir que se sobrescriban las etiquetas de IBM Spectrum Protect, lo que podría provocar la pérdida de datos, asegúrese de que sólo el controlador Passthru de IBM Spectrum Protect controle los dispositivos utilizados por IBM Spectrum Protect. Elimine el controlador st del kernel o, si el controlador es utilizado por algunas aplicaciones del sistema, suprima los archivos especiales que se corresponden con los dispositivos de IBM Spectrum Protect de modo que el controlador st ya no pueda controlarlos.

Si utiliza el controlador de dispositivo de cinta de IBM para controlar los dispositivos del sistema, puede encontrar los mismos problemas con conflictos en el control de los controladores de dispositivos. Revise la documentación sobre cintas de IBM para determinar cómo resolver este problema y prevenir la pérdida de datos.

### Eliminar el controlador st

Si no hay ninguna otra aplicación en el sistema que utilice dispositivos st, elimine el controlador st del kernel. Emita el siguiente mandato para descargar el controlador st:

```
rmmod st
```

### Suprima los archivos especiales de dispositivo que se correspondan con dispositivos de IBM Spectrum Protect

Si hay aplicaciones que requieren el uso del controlador st, suprima los archivos especiales que corresponden a dispositivos de IBM Spectrum Protect. Estos archivos especiales los genera por el controlador st. Cuando se eliminan, el controlador st ya no puede controlar los dispositivos de IBM Spectrum Protect correspondientes. Los nombres de archivos especiales de dispositivo para unidades de cinta aparecen en el directorio /dev/. Sus nombres tienen el formato /dev/[n]st[0-1024][l][m][a].


Enumere los nombres del archivo especial de la unidad st y los nombres del archivo especial del dispositivo IBM Spectrum Protect al usar el mandato ls. Basándose en la salida de las secuencias del dispositivo, puede encontrar dispositivos en la lista de dispositivos st que coincidan con los de la lista de dispositivos de IBM Spectrum Protect. El mandato rm puede utilizarse a continuación para suprimir dispositivos st.

Emita los siguientes mandatos para listar los dispositivos st y de IBM Spectrum Protect:

```
ls -l /dev/*st*
ls -l /dev/tmsmcsi/mt*
```

Suprima los dispositivos st con el mandato rm:



```
rm /dev/*st*
```


 Sistemas operativos Windows

## Configuración de controladores de dispositivos de cinta en sistemas Windows

---

Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta y bibliotecas en sistemas Windows.

-  **Sistemas operativos Windows** Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta  
Para utilizar el controlador de dispositivo de paso a través de IBM Spectrum Protect Windows para bibliotecas y dispositivos de cinta, debe instalar el controlador y obtener los nombres de dispositivos para que los use el servidor.
-  **Sistemas operativos Windows** Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta  
Si el fabricante de una unidad de cintas o biblioteca de cintas no proporciona un controlador de dispositivos SCSI, debe instalar el controlador de dispositivos IBM Spectrum Protect SCSI.

 Sistemas operativos Windows



# Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta

Para utilizar el controlador de dispositivo de paso a través de IBM Spectrum Protect Windows para bibliotecas y dispositivos de cinta, debe instalar el controlador y obtener los nombres de dispositivos para que los use el servidor.

## Antes de empezar

1. Determine si el fabricante del dispositivo de cinta o biblioteca de cintas proporciona un controlador de dispositivo.
2. Si el fabricante proporciona un paquete de controlador de dispositivo, descargue el paquete e instálelo.
3. Configure el controlador de dispositivo SCSI siguiendo las instrucciones del fabricante.

## Procedimiento

1. Instale el controlador del dispositivo de paso a través de IBM Spectrum Protect.
2. Obtenga los nombres de dispositivo que el servidor debe utilizar realizando una de las siguientes acciones:
  - En el servidor, ejecute el mandato QUERY SAN. La salida muestra todos los nombres de dispositivo y los números de serie de dispositivo asociados.
  - En el directorio del servidor ejecute el programa de utilidad tsmdlst.exe. La salida muestra todos los nombres de dispositivos, sus números de serie asociados y las ubicaciones de dispositivo asociadas.
  - En el indicador de mandatos del sistema Windows, ejecute el mandato regedit. Desde la salida, obtenga los nombres de archivos de dispositivo en función de las ubicaciones de los dispositivos. La ubicación consta de ID de puerto, ID de bus de SCSI, ID de LUN ID e ID de destino de SCSI. El nombre de archivo de dispositivo de IBM Spectrum Protect tiene un formato mtA.B.C.C para unidades de cinta y lbA.B.C.D para bibliotecas de cinta, donde:
    - A es el ID de destino de SCSI.
    - B es el ID de LUN.
    - C es el ID de bus de SCSI.
    - D es el ID de puerto.

 Sistemas operativos Windows

## Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta

Si el fabricante de una unidad de cintas o biblioteca de cintas no proporciona un controlador de dispositivos SCSI, debe instalar el controlador de dispositivos IBM Spectrum Protect SCSI.

## Acerca de esta tarea

El nombre de archivo de controlador de dispositivo SCSI de IBM Spectrum Protect es tsmcsi64.sys.

## Procedimiento

1. Localice el dispositivo en la consola del gestor de dispositivos (devmgmt.msc) y selecciónelo. Las unidades de cinta se listan en Unidades de cinta, y los conmutadores de soporte en Conmutadores de soporte.
2. Configure el dispositivo para que lo utilice el controlador de dispositivo tsmcsi64.sys:
  - a. Pulse con el botón derecho sobre el dispositivo y pulse Actualizar software de controlador.
  - b. Pulse Buscar software de controlador en el equipo.
3. Pulse Elegir en una lista de controladores de dispositivo en mi PC.
4. Pulse Siguiente.
5. Seleccione la opción adecuada:
  - a. Para una unidad de cintas, seleccione IBM Spectrum Protect para unidades de cinta.
  - b. Para un conmutador de soporte, seleccione IBM Spectrum Protect para conmutadores de soporte.
6. Pulse Siguiente.
7. Pulse Cerrar.
8. Compruebe que el dispositivo se ha configurado correctamente para el controlador de dispositivo tsmcsi64:
  - a. Pulse con el botón derecho sobre el dispositivo y pulse Propiedades.
  - b. Pulse el separador Controlador y Detalles de controlador. La ventana Detalles de controlador muestra el controlador de dispositivo que controla el dispositivo.

# Configuración de bibliotecas para su uso por parte de un servidor

Para utilizar una biblioteca o bibliotecas para el almacenamiento de un servidor de IBM Spectrum Protect, primero tiene que configurar los dispositivos en el sistema servidor.

## Antes de empezar

1. Conecte los dispositivos al hardware del servidor. Siga las instrucciones que encontrará en Conectar un dispositivo de biblioteca automática a su dispositivo.
2. Seleccione los controladores de dispositivo de cinta. Siga las instrucciones que encontrará en Seleccionar un controlador de dispositivo de cinta.
3. Instale y configure los controladores de dispositivo de cinta. Siga las instrucciones que encontrará en Instalación y configuración de controladores de dispositivos de cinta.
4. Determine los nombres de dispositivo que se necesitan para definir la biblioteca en el servidor. Siga las instrucciones que encontrará en Nombres de archivo especiales para dispositivos de cinta.

## Procedimiento

1. Defina la biblioteca y la vía de acceso desde el servidor a la biblioteca. Siga las instrucciones que encontrará en Definición de bibliotecas.
2. Defina las unidades en la biblioteca. Siga las instrucciones que encontrará en Definición de unidades.

Para las bibliotecas SCSI, puede utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca en un solo paso, en lugar de completar los dos pasos 2 y 3. Para utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca, la opción `SANDISCOVERY` debe estar admitida y habilitada.

3. Defina una vía de acceso desde el servidor a cada unidad mediante el mandato `DEFINE PATH`.
4. Defina una clase de dispositivo. Siga las instrucciones que encontrará en Definición de las clases de dispositivo de cinta.

Las clases de dispositivo especifican los formatos de grabación para las unidades y las clasifican según el tipo. Utilice el valor predeterminado, `FORMAT=DRIVE`, como formato de grabación solo si todas las unidades asociadas a la clase de dispositivo pueden leer y grabar en todos los medios.

Por ejemplo, imagine que tiene una mezcla de unidades Ultrium generación 3 y Ultrium generación 4, pero solo tiene medios Ultrium generación 3. Puede especificar `FORMAT=DRIVE` porque tanto las unidades Generación 4 como las unidades Generación 3 pueden leer y grabar en medios de Generación 3. media.

5. Definir una agrupación de almacenamiento con el mandato `DEFINE STGPOOL`.

Tenga en cuenta las siguientes opciones clave para definir agrupaciones de almacenamiento:

- Los volúmenes reutilizables son volúmenes vacíos que están disponibles para el uso. Si especifica un valor para el máximo número de volúmenes reutilizables en la agrupación de almacenamiento, el servidor puede elegir entre los volúmenes reutilizables disponibles en la biblioteca.

Si no permite los volúmenes reutilizables, debe completar el paso adicional de definir explícitamente cada volumen que se utilizará en la agrupación de almacenamiento. Además, especifique el parámetro `MAXSCRATCH=0` al definir la agrupación de almacenamiento para que no se utilicen los volúmenes reutilizables.

- El valor predeterminado de las agrupaciones de almacenamiento primarias es la proximidad por grupo. El valor predeterminado para agrupación de almacenamiento de copias y agrupaciones de datos activos es la desactivación de la proximidad. El servidor utiliza la *proximidad* para mantener todos los archivos que pertenecen a un grupo de nodos cliente, a un solo nodo cliente, a un espacio de archivos de cliente o a un grupo de espacio de archivos de cliente en el mínimo número de volúmenes. Si se desactiva la proximidad para una agrupación de almacenamiento y los clientes comienzan a almacenar datos, no podrá cambiar fácilmente los datos de la agrupación de forma que éstos sigan estando próximos entre sí.

6. Dé de alta y etiquete los volúmenes de la biblioteca. Siga las instrucciones que encontrará en Incorporar volúmenes en una biblioteca automatizada y Etiquetado de volúmenes de cinta.

Asegúrese de que haya suficientes volúmenes disponibles para el servidor. Tenga siempre a mano un número suficiente de volúmenes etiquetados de manera que no le falten cuando realice operaciones importantes, como por ejemplo, la copia de seguridad de los clientes. Etiquete volúmenes reutilizables adicionales para posibles operaciones de recuperación que puedan surgir posteriormente.

Los procedimientos para dar de alta y etiquetar volúmenes son los mismos tanto si la biblioteca contiene unidades de un solo tipo de dispositivo como si son de varios tipos de dispositivo. Puede utilizar el mandato `CHECKIN LIBVOLUME` para dar de alta volúmenes que ya están etiquetados. O, si desea etiquetar y dar de alta volúmenes con un solo paso, emita el mandato `LABEL LIBVOLUME`.

Bibliotecas con varios tipos de dispositivo: Si la biblioteca tiene unidades de varios tipos de dispositivo y ha definido dos bibliotecas en el servidor de IBM Spectrum Protect, las dos bibliotecas definidas representan una biblioteca física. Debe dar de alta los volúmenes de cinta por separado en cada biblioteca definida. Asegúrese de dar de alta los volúmenes en la biblioteca de IBM Spectrum Protect correcta.

## Qué hacer a continuación

---

Compruebe las definiciones de dispositivos para asegurarse de que todo está configurado correctamente. Utilice un mandato QUERY para revisar la información sobre cada objeto de almacenamiento.

Al revisar los resultados del mandato QUERY DRIVE, verifique que el tipo de dispositivo para la unidad es el esperado. Si no se ha definido una vía de acceso, el tipo de dispositivo de unidad se lista como UNKNOWN y si se utiliza la vía de acceso equivocada, se muestra GENERIC\_TAPE u otro tipo de dispositivo. Este paso es especialmente importante cuando se utilizan medios mezclados.

Opcionalmente, configure la compartición de bibliotecas. Siga las instrucciones que encontrará en Configuración de la compartición de bibliotecas.

- Definición de dispositivos de cinta  
Antes de realizar una copia de seguridad o migrar datos a la cinta, debe definir un dispositivo de cinta en IBM Spectrum Protect.
- Configuración de la compartición de bibliotecas  
Varios servidores de IBM Spectrum Protect pueden compartir dispositivos de almacenamiento por medio de una red de área de almacenamiento (SAN). Se debe configurar un servidor como gestor de biblioteca y los demás servidores como clientes de biblioteca.

### Referencia relacionada:

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- ➔ PERFORM LIBACTION (Definir o suprimir todas las unidades y las vías de acceso de una biblioteca)

### Información relacionada:

- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Definición de dispositivos de cinta

---

Antes de realizar una copia de seguridad o migrar datos a la cinta, debe definir un dispositivo de cinta en IBM Spectrum Protect.

- Definición de bibliotecas y unidades  
Una biblioteca de cintas puede incluir una o más unidades de cinta. Aprenda a definir bibliotecas, unidades y vías de acceso para el servidor IBM Spectrum Protect.
- Definición de las clases de dispositivo de cinta  
Una clase de dispositivo define un conjunto de características que utiliza un conjunto de volúmenes que se pueden crear en una agrupación de almacenamiento. Debe definir una clase de dispositivo para un dispositivo de cinta para asegurarse de que el servidor puede utilizar el dispositivo.

## Definición de bibliotecas y unidades

---

Una biblioteca de cintas puede incluir una o más unidades de cinta. Aprenda a definir bibliotecas, unidades y vías de acceso para el servidor IBM Spectrum Protect.

- Definición de bibliotecas  
Para poder utilizar una unidad, debe definir la biblioteca a la que pertenece.
- Definición de unidades  
Para informar al servidor con respecto a una unidad que puede utilizarse para acceder a los volúmenes de almacenamiento, emita el mandato DEFINE DRIVE, seguido del mandato DEFINE PATH.

## Definición de bibliotecas

---

Para poder utilizar una unidad, debe definir la biblioteca a la que pertenece.

### Procedimiento

---

1. Defina la biblioteca utilizando el mandato DEFINE LIBRARY.


Por ejemplo, si tiene una biblioteca de cintas IBM TS3500, puede definir una biblioteca denominada ROBOTMOUNT con el siguiente mandato:

```
define library robotmount libtype=scsi
```


Si necesita la compartición de biblioteca o el movimiento de datos sin LAN, consulte la siguiente información:

- Configuración de la compartición de bibliotecas
- Configuración del movimiento de datos sin LAN


2. Defina una vía de acceso desde el servidor a la biblioteca mediante el mandato DEFINE PATH. Cuando especifique el parámetro DEVICE, escriba el nombre del archivo especial de dispositivo. El servidor necesita este nombre para comunicarse con las unidades de cinta, el conmutador de soporte y los dispositivos de soporte extraíbles. Para obtener más información sobre los nombres de archivos especiales de dispositivo, consulte Nombres de archivo especiales para dispositivos de cinta.

 Sistemas operativos AIX

```
define path server1 robotmount srctype=server desttype=library
device=/dev/lb0
```

 Sistemas operativos Linux

```
define path server1 robotmount srctype=server desttype=library
device=/dev/tsm SCSI/lb0
```


 Sistemas operativos Windows


```
define path server1 robotmount srctype=server desttype=library
device=lb0.0.1.0
```

- Definición de bibliotecas SCSI en una SAN

En el caso de un tipo de biblioteca SCSI en una SAN, el servidor puede hacer el seguimiento del número de serie de la biblioteca. Con el número de serie, el servidor puede confirmar la identidad del dispositivo al definir la vía de acceso o cuando el servidor utilice el dispositivo.

#### Información relacionada:

 [DEFINE LIBRARY \(Definir una biblioteca\)](#)

 [DEFINE PATH \(Definir una vía de acceso\)](#)

## Definición de unidades

---

Para informar al servidor con respecto a una unidad que puede utilizarse para acceder a los volúmenes de almacenamiento, emita el mandato DEFINE DRIVE, seguido del mandato DEFINE PATH.

### Antes de empezar

---

Un *objeto de unidad* representa un mecanismo de unidad en una biblioteca que usa soportes de almacenamiento extraíbles. En el caso de dispositivos con varias unidades, incluidas las bibliotecas automatizadas, se debe definir cada unidad por separado y asociarla con una biblioteca. Las definiciones de unidad pueden incluir información como, por ejemplo, la dirección del elemento para las unidades en SCSI, la frecuencia con que se limpia una unidad de cintas y si la unidad está en línea.

IBM Spectrum Protect da soporte a las unidades de cinta que pueden ser autónomas o pueden formar parte de una biblioteca automatizada. El método preferido consiste en configurar la solución de cinta utilizando bibliotecas automatizadas.

### Acerca de esta tarea

---

Al emitir el mandato DEFINE DRIVE, debe proporcionar alguno o todos los datos de la siguiente información:

Nombre de biblioteca

El nombre de la biblioteca en la que se encuentra la unidad.

Nombre de unidad

El nombre que se ha asignado a la unidad.

Número de serie

El número de serie de la unidad. El parámetro de número de serie sólo es válido para las unidades de SCSI. Con el número de serie, el servidor puede confirmar la identidad del dispositivo al definir la vía de acceso o cuando el servidor utilice el dispositivo.

Si lo desea, puede especificar el número de serie. El valor predeterminado consiste en permitir al servidor obtener el número de serie de la propia unidad al definirse la vía de acceso. Si especifica el número de serie, el servidor confirma que el número de serie es correcto al definir la vía de acceso para la unidad. Al definir la vía de acceso, puede establecer el parámetro AUTODETECT=YES para permitir al servidor corregir el número de serie si el número que detecta no coincide con el especificado

al definir la unidad. Como práctica recomendada, especifique el parámetro AUTODETECT=YES para actualizar automáticamente el número de serie para la unidad en la base de datos al definir la vía de acceso.

Según las posibilidades de la unidad, es posible que el servidor no pueda detectar automáticamente el número de serie. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo. Consulte el apartado Influencia de los cambios de dispositivo en la SAN.

#### Dirección de elemento

La dirección de elemento de la unidad. El parámetro ELEMENT se aplica solo a las unidades de las bibliotecas SCSI. La dirección de elemento es un número que indica la ubicación física de una unidad en una biblioteca automatizada. El servidor necesita la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. El servidor puede obtener la dirección de elemento desde la unidad al definir la vía de acceso, o puede especificar el número de elemento al definir la unidad. Como práctica recomendada, especifique el parámetro ELEMENT=AUTODETECT para que el servidor detecte automáticamente el número de elemento cuando se defina la vía de acceso a la unidad.

Según las capacidades de la biblioteca, es posible que el servidor no pueda detectar automáticamente la dirección de elemento. En ese caso, deberá proporcionar la dirección de elemento al definir la unidad, si la biblioteca tiene más de una unidad. Para obtener la dirección de elemento, vaya a IBM® Support Portal for IBM Spectrum Protect.

Consejo: Los controladores de dispositivo de cinta de IBM y los controladores de dispositivo de cinta no IBM generan distintos archivos y formatos de dispositivo:

- Para IBM, los nombres de dispositivos empiezan por rmt seguido de un entero, por ejemplo, /dev/rmt0.
- Para los controladores de dispositivo de cinta de IBM Spectrum Protect, los nombres de controlador de dispositivo de cinta empiezan por mt seguido de un entero, por ejemplo /dev/mt0.

Debe utilizar el archivo de dispositivo correcto cuando defina una vía de acceso.

## Procedimiento

---

1. asigne una unidad a la biblioteca emitiendo el mandato DEFINE DRIVE.
2. Para que el servidor pueda utilizar la unidad, emita el mandato DEFINE PATH.

Para ejemplos sobre la configuración de bibliotecas, vías de acceso y unidades, consulte Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad y Ejemplo: Configurar una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad.

## Definición de las clases de dispositivo de cinta

---

Una clase de dispositivo define un conjunto de características que utiliza un conjunto de volúmenes que se pueden crear en una agrupación de almacenamiento. Debe definir una clase de dispositivo para un dispositivo de cinta para asegurarse de que el servidor puede utilizar el dispositivo.

## Antes de empezar




---

Debe definir las bibliotecas y unidades en el servidor antes de definir las clases de dispositivo.

## Acerca de esta tarea

---

Para obtener una lista de dispositivos soportados y formatos de clase de dispositivo válidos, consulte el sitio web Dispositivos soportados de IBM Spectrum Protect para su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos soportados para AIX y Windows
-  Sistemas operativos Linux Dispositivos soportados para Linux

Se pueden definir varias clases de dispositivo para cada tipo de dispositivo. Por ejemplo, es posible que necesite especificar distintos atributos para distintas agrupaciones de almacenamiento que utilizan el mismo tipo de unidad de cintas. Es posible que se requieran variaciones que no son específicas para el dispositivo, sino de la forma en que se desea utilizar el dispositivo (por ejemplo, la retención o el límite de montaje).

Directrices:

- Una clase de dispositivo puede asociarse con varias agrupaciones de almacenamiento, pero cada agrupación de almacenamiento puede estar asociada sólo con una clase de dispositivo.

- Las bibliotecas SCSI puede incluir unidades de cinta de más de un tipo de dispositivo. Al definir la clase de dispositivo en este entorno, debe declarar un valor para el parámetro FORMAT.

Para obtener más información, consulte Mezcla de tipos de dispositivos en una biblioteca.

## Procedimiento

Para definir una clase de dispositivo, utilice el mandato DEFINE DEVCLASS con el parámetro DEVTYPE, que asigna un tipo de dispositivo a la clase de dispositivo.

## Resultados

Si incluye la opción DEVCONFIG del archivo dsmserv.opt, los archivos que especifique con esa opción se actualizan automáticamente con los resultados de los mandatos DEFINE DEVCLASS, UPDATE DEVCLASS y DELETE DEVCLASS.

- **Definición de las clases de dispositivo LTO**  
Para evitar problemas a la hora de combinar distintas generaciones de unidades y medios LTO en una sola biblioteca, revise las restricciones. Revise también las restricciones para el cifrado de unidad LTO.
- **Definición de clases de dispositivo 3592**  
Las definiciones de clase de dispositivo para 3592, TS1130, TS1140, TS1150 y dispositivos posteriores incluyen parámetros para una mayor velocidad de acceso a los volúmenes y un cifrado de unidad más rápido. Para evitar que se produzcan problemas al mezclar distintas generaciones de 3592 y TS1130 y unidades posteriores de una biblioteca, revise las directrices.

### Referencia relacionada:

[DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

### Información relacionada:

[QUERY DEVCLASS \(Visualizar información en una o más clases de dispositivo\)](#)

[UPDATE DEVCLASS \(Actualizar una clase de dispositivo\)](#)

## Definición de las clases de dispositivo LTO

Para evitar problemas a la hora de combinar distintas generaciones de unidades y medios LTO en una sola biblioteca, revise las restricciones. Revise también las restricciones para el cifrado de unidad LTO.

- **Combinación de unidades y medios LTO en una biblioteca**  
Al combinar diferentes generaciones de unidades y medios LTO, debe tener en cuenta las funcionalidades de lectura-grabación de cada generación. El método preferido consiste en configurar diferentes clases de dispositivo para cada generación de medios.
- **Límites de montaje en entornos de medios mixtos LTO**  
En una biblioteca con medios mixtos, en la que varias clases de dispositivo hacen referencia a la misma biblioteca, las unidades compatibles se comparten entre las agrupaciones de almacenamiento. Asegúrese de establecer un valor adecuado para el parámetro MOUNTLIMIT en cada una de las clases de dispositivo.
- **Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior**  
IBM Spectrum Protect admite los tres tipos de cifrado de unidad disponibles con las unidades LTO generación 4 o posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

## Combinación de unidades y medios LTO en una biblioteca

Al combinar diferentes generaciones de unidades y medios LTO, debe tener en cuenta las funcionalidades de lectura-grabación de cada generación. El método preferido consiste en configurar diferentes clases de dispositivo para cada generación de medios.

### Acerca de esta tarea

Si piensa en mezclar distintas generaciones de unidades y medios LTO, revise las siguientes restricciones:

Tabla 1. Funcionalidades de lectura/grabación para distintas generaciones de unidades LTO

| Unidades     | Medios de la generación 1   | Medios de la generación 2 | Medios de la generación 3 | Medios de la generación 4 | Medios de la generación 5 | Medios de la generación 6 | Medios de la generación 7 |
|--------------|-----------------------------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| Generación 1 | Acceso de lectura/escritura | n/d                       | n/d                       | n/d                       | n/d                       | n/d                       | n/d                       |

| Unidades     | Medios de la generación 1   | Medios de la generación 2   | Medios de la generación 3   | Medios de la generación 4   | Medios de la generación 5   | Medios de la generación 6   | Medios de la generación 7   |
|--------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| Generación 2 | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         | n/d                         | n/d                         | n/d                         |
| Generación 3 | Acceso de solo lectura      | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         | n/d                         | n/d                         |
| Generación 4 | n/d                         | Acceso de solo lectura      | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         | n/d                         |
| Generación 5 | n/d                         | n/d                         | Acceso de solo lectura      | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         |
| Generación 6 | n/d                         | n/d                         | n/d                         | Acceso de solo lectura      | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         |
| Generación 7 | n/d                         | n/d                         | n/d                         | n/d                         | Acceso de lectura           | Acceso de lectura/escritura | Acceso de lectura/escritura |

## Ejemplo

Si combina diferentes tipos de unidades y medios, configure diferentes clases de dispositivo: una para cada tipo de medio. Para especificar el tipo de medio, utilice el parámetro FORMAT en cada una de las definiciones de clase de dispositivo. (No especifique FORMAT=DRIVE.) Por ejemplo, si combina unidades Ultrium generación 5 y Ultrium generación 6, especifique FORMAT=ULTRIUM5C (o ULTRIUM5) para la clase de dispositivo Ultrium generación 5, y FORMAT=ULTRIUM6C (o ULTRIUM6) para la clase de dispositivo Ultrium generación 6.

En este ejemplo, ambas clases de dispositivos pueden apuntar a la misma biblioteca con las unidades Ultrium generación 5 y Ultrium generación 6. Las unidades se compartirán entre las dos agrupaciones de almacenamiento. Una agrupación de almacenamiento utilizará exclusivamente la primera clase de dispositivo y el medio Ultrium generación 5. La otra agrupación de almacenamiento utilizará exclusivamente la segunda clase de dispositivo y el medio Ultrium generación 6. Puesto que las dos agrupaciones de almacenamiento comparten una única biblioteca, los medios Ultrium generación 5 pueden montarse en unidades Ultrium generación 6 a medida que vayan estando disponibles durante el procesamiento de puntos de montaje.

Si combina generaciones de soportes de sólo lectura más antiguos con soportes de lectura/escritura más nuevos en una única biblioteca, deberá marcar los soportes de sólo lectura como sólo lectura y extraer todos los soportes reutilizables de sólo lectura. Por ejemplo, si combina unidades y medios Ultrium generación 4 con Ultrium generación 6 en una sola biblioteca, debe marcar los medios de generación 4 como solo lectura. Además, debe extraer todos los volúmenes reutilizables de generación 4.

## Límites de montaje en entornos de medios mixtos LTO

En una biblioteca con medios mixtos, en la que varias clases de dispositivo hacen referencia a la misma biblioteca, las unidades compatibles se comparten entre las agrupaciones de almacenamiento. Asegúrese de establecer un valor adecuado para el parámetro MOUNTLIMIT en cada una de las clases de dispositivo.

Por ejemplo, en una biblioteca de medios mixta que contenga unidades y medios Ultrium Generation 1 y Ultrium Generation 2, por ejemplo, los medios Ultrium Generation 1 pueden montarse en unidades Ultrium Generation 2.

Suponga un ejemplo de una biblioteca mixta que conste de los siguientes medios y unidades:

- Cuatro unidades LTO Ultrium Generation 1 y medios LTO Ultrium Generation 1.
- Cuatro unidades LTO Ultrium Generation 2 y medios LTO Ultrium Generation 2.

Se crearon las clases de dispositivo siguientes:

- Clase de dispositivo de LTO Ultrium Generation 1 LTO1CLASS, especificando FORMAT=ULTRIUMC
- Clase de dispositivo de LTO Ultrium Generation 2 LTO2CLASS, especificando FORMAT=ULTRIUM2C

También se crearon las agrupaciones de almacenamiento siguientes:

- Agrupación de almacenamiento LTO Ultrium Generation 1 LTO1POOL basada en la clase de dispositivo LTO1CLASS.
- Agrupación de almacenamiento LTO Ultrium Generation 2 LTO2POOL basada en la clase de dispositivo LTO2CLASS.

El número de puntos de montaje disponibles para que utilice cada agrupación de almacenamiento se especifica en la clase de dispositivo utilizando el parámetro MOUNTLIMIT. El parámetro MOUNTLIMIT de la clase de dispositivo LTO2CLASS debe estar establecido en 4 para que coincida con el número de unidades disponibles que solo pueden montar medios LTO2. El parámetro MOUNTLIMIT de la clase de dispositivo LTO1CLASS debe estar establecido en un valor que sea mayor que el número de unidades disponibles (5 o posiblemente 6) para tener en cuenta que los medios Ultrium Generation 1 pueden montarse en unidades Ultrium Generation 2. El valor óptimo de MOUNTLIMIT depende de los patrones de acceso de la carga de trabajo y la agrupación de almacenamiento.

Supervise y ajuste el valor de MOUNTLIMIT para adecuarlo a las cargas de trabajo cambiantes. Si MOUNTLIMIT para LTO1POOL se establece en un valor demasiado alto, es posible que las solicitudes de montaje de LTO2POOL se retrasen o fallen, ya que se han utilizado las unidades Ultrium Generation 2 para satisfacer las solicitudes de montaje de medios Ultrium Generation 1. En el peor de los casos, demasiada competencia para las unidades Ultrium Generation 2 puede provocar el siguiente error en los montajes de medios Generation 2:

```
ANR8447E No
hay unidades disponibles en este momento en la biblioteca.
```

Si el valor de MOUNTLIMIT para LTO1POOL no está establecido lo suficientemente alto, se retrasan las solicitudes de montaje de unidades LTO Ultrium Generation 2 que se podrían satisfacer.

Restricción: Se aplican restricciones al combinar unidades Ultrium Generation 1 con unidades Ultrium Generation 2 o Generation 3 debido a la forma en que están asignados los puntos de montaje. Por ejemplo, es posible que aquellos procesos que requieran varios puntos de montaje que incluyan volúmenes tanto Ultrium Generation 1 como Ultrium Generation 2 intenten reservar sólo unidades Ultrium Generation 2 aunque una unidad Ultrium Generation 1 disponible podría satisfacer un montaje. Entre los procesos que se comportan así se incluyen los mandatos MOVE DATA y BACKUP STGPOOL. Estos procesos esperarán hasta que se pueda satisfacer la cantidad necesaria de puntos de montaje con unidades Ultrium Generation 2.

**Referencia relacionada:**

- BACKUP STGPOOL (Hacer copia de seguridad de los datos de la agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia)
- DEFINE DEVCLASS (Definir una clase de dispositivo)
- MOVE DATA (Trasladar archivos a un volumen de agrupación de almacenamiento)

## Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior

IBM Spectrum Protect admite los tres tipos de cifrado de unidad disponibles con las unidades LTO generación 4 o posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

### Acerca de esta tarea

El parámetro DRIVEENCRYPTION del mandato DEFINE DEVCLASS especifica si se permite el cifrado de unidad para unidades IBM y HP LTO generación 4 o posterior, formatos Ultrium 4 y Ultrium 4C. Este parámetro garantiza la compatibilidad de IBM Spectrum Protect con los valores de cifrado de hardware para volúmenes vacíos. No puede utilizar este parámetro para los volúmenes de agrupaciones de almacenamiento que estén llenos o se estén llenando.

IBM Spectrum Protect admite el método de Aplicación de cifrado con unidades IBM y HP LTO-4 o posteriores. Solo IBM LTO-4 o posterior admite los métodos Sistema y Biblioteca. El método de cifrado Biblioteca solo se puede utilizar si el hardware del sistema (por ejemplo IBM TS3500) lo admite.

Restricción: No puede utilizar el cifrado de unidades con medios WORM (grabar una vez leer muchas).

El método de Aplicación se define mediante el hardware. Para utilizar el método de aplicación en el que IBM Spectrum Protect genera y gestiona claves de cifrado, establezca el parámetro DRIVEENCRYPTION en ON. Esta acción habilita el cifrado de datos para volúmenes vacíos. Si el parámetro se establece en ON y el hardware está configurado para otro método de cifrado, las operaciones de copia de seguridad fallan.

### Procedimiento

En el ejemplo simplificado siguiente se muestran los pasos que es preciso seguir para habilitar o inhabilitar el cifrado de datos para volúmenes vacíos en una agrupación de almacenamiento:

1. Defina una biblioteca emitiendo el mandato DEFINE LIBRARY:



```
define library 3584 libtype=SCSI
```

2. Defina una clase de dispositivo, LTO\_ENCRYPT, emitiendo el mandato DEFINE DEVCLASS y especificando IBM Spectrum Protect como gestor de claves:

```
define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
```

3. Definir una agrupación de almacenamiento emitiendo el mandato DEFINE STGPOOL:

```
define stgpool lto_encrypt_pool lto_encrypt
```

4. Para inhabilitar el cifrado en volúmenes nuevos, establezca el parámetro DRIVEENCRYPTION con el valor OFF. El valor predeterminado es ALLOW. Se permite el cifrado de unidades de volúmenes vacíos si se ha habilitado otro método de cifrado.

#### Conceptos relacionados:

Métodos de cifrado de cinta

## Definición de clases de dispositivo 3592

Las definiciones de clase de dispositivo para 3592, TS1130, TS1140, TS1150 y dispositivos posteriores incluyen parámetros para una mayor velocidad de acceso a los volúmenes y un cifrado de unidad más rápido. Para evitar que se produzcan problemas al mezclar distintas generaciones de 3592 y TS1130 y unidades posteriores de una biblioteca, revise las directrices.

- Combinación de generaciones de unidades y medios 3592 en una sola biblioteca  
Para obtener un rendimiento óptimo, no combine generaciones de medios 3592 en una sola biblioteca. Pueden producirse problemas al mezclarse diferentes generaciones de medios. Por ejemplo, puede que IBM Spectrum Protect no sea capaz de leer la etiqueta de un volumen.
- Control de las velocidades de acceso a datos en volúmenes 3592  
Puede optimizar la capacidad de almacenamiento y mejorar la velocidad de acceso al crear volúmenes. Al particionar datos en agrupaciones de almacenamiento que tienen volúmenes, puede especificar el porcentaje de capacidad de escala para proporcionar la máxima capacidad de almacenamiento o para proporcionar un acceso rápido al volumen.
- Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior  
Con IBM Spectrum Protect, puede utilizar los siguientes tipos de cifrados de unidad con unidades que sean 3592 generación 2 y posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

## Combinación de generaciones de unidades y medios 3592 en una sola biblioteca

Para obtener un rendimiento óptimo, no combine generaciones de medios 3592 en una sola biblioteca. Pueden producirse problemas al mezclarse diferentes generaciones de medios. Por ejemplo, puede que IBM Spectrum Protect no sea capaz de leer la etiqueta de un volumen.

### Acerca de esta tarea

En la tabla siguiente se muestra la interoperatividad de lectura-grabación para las generaciones de unidades.

| Unidades     | Formato de Generación 1     | Formato de Generación 2     | Formato de Generación 3     | Formato de Generación 4     | Formato de Generación 5     |
|--------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| Generación 1 | Acceso de lectura/escritura | n/d                         | n/d                         | n/d                         | n/d                         |
| Generación 2 | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         | n/d                         |
| Generación 3 | Acceso de solo lectura      | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         | n/d                         |
| Generación 4 | n/d                         | Sólo lectura                | Acceso de lectura/escritura | Acceso de lectura/escritura | n/d                         |
| Generación 5 | n/d                         | n/d                         | Acceso de lectura           | Acceso de lectura/escritura | Acceso de lectura/escritura |

Si debe combinar generaciones de unidades en una biblioteca, revise el ejemplo y las restricciones para evitar problemas.

Tabla 1. Combinación de generaciones de unidades

| Tipo de biblioteca | Ejemplo y restricciones                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SCSI               | <p>Define una nueva agrupación de almacenamiento y clase de dispositivo para la última generación de unidad. Por ejemplo, supongamos que tiene una agrupación de almacenamiento y una clase de dispositivo para 3592-2. La agrupación de almacenamiento contiene todos los medios que se han grabado en formato Generación 2. Supongamos que el valor del parámetro FORMAT en la definición de clase de dispositivo se establece en 3952-2 (no en DRIVE). Añada unidades de Generación 3 a la biblioteca. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la nueva definición de clase de dispositivo para las unidades de generación 3, establezca el valor del parámetro FORMAT en 3592-3 o 3592-3C. No especifique DRIVE.</li> <li>2. En la definición de la agrupación de almacenamiento asociada con las unidades de generación 2, actualice el parámetro MAXSCRATCH a 0, por ejemplo:</li> </ol> <pre>update stgpool genpool2 maxscratch=0</pre> <p>Este método permite que ambas generaciones utilicen su formato óptimo y se minimicen los posibles problemas de medios que puedan producirse como consecuencia de combinar generaciones. No obstante, no solucionará todos los problemas de medios. Por ejemplo, pueden darse casos de competencia por los puntos de montaje y que se produzcan anomalías de montaje. (para obtener información sobre cómo completar puntos de montaje en el contexto de unidades y medios 3592, consulte Definición de clases de dispositivo 3592.)</p> <p>Restricción: La siguiente lista describe las restricciones de medios:</p> <ul style="list-style-type: none"> <li>• CHECKIN LIBVOL: El problema radica en la utilización de la opción CHECKLABEL=YES. Si la etiqueta está escrita actualmente en un formato de generación 3 o posterior y especifica la opción CHECKLABEL=YES, las unidades de las generaciones anteriores fallan si utilizan este mandato. Para evitar el problema, especifique CHECKLABEL=BARCODE.</li> <li>• LABEL LIBVOL: Cuando el servidor intenta utilizar unidades de una generación anterior para leer la etiqueta escrita con un formato de generación 3 o posterior, el mandato LABEL LIBVOL falla a menos que se especifique OVERWRITE=YES. Verifique que el soporte que se está etiquetando con OVERWRITE=YES no tiene datos activos.</li> <li>• CHECKOUT LIBVOL: Cuando IBM Spectrum Protect verifica la etiqueta (CHECKLABEL=YES), como un formato de generación 3 o posterior, y lee unidades de generaciones anteriores, el mandato falla. Para evitar este problema, especifique CHECKLABEL=NO.</li> </ul> |

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

## Control de las velocidades de acceso a datos en volúmenes 3592

Puede optimizar la capacidad de almacenamiento y mejorar la velocidad de acceso al crear volúmenes. Al particionar datos en agrupaciones de almacenamiento que tienen volúmenes, puede especificar el porcentaje de capacidad de escala para proporcionar la máxima capacidad de almacenamiento o para proporcionar un acceso rápido al volumen.

### Acerca de esta tarea

Para reducir la capacidad de un medio, especifique el parámetro SCALECAPACITY cuando defina la clase de dispositivo utilizando el mandato DEFINE DEVCLASS o cuando actualice la clase de dispositivo utilizando el mandato UPDATE DEVCLASS.

Especifique un valor de porcentaje de 20, 90 o 100. Un valor de 20% proporciona el tiempo de acceso más rápido y un valor de 100% proporciona la mayor capacidad de almacenamiento. Por ejemplo, si especifica una capacidad de escala de 20 para una clase de dispositivo 3592 sin compresión, un volumen 3592 en esa clase de dispositivo almacenaría el 20 por ciento de su capacidad total de 300 GB, cerca de 60 GB.

El valor de la capacidad de escala sólo entra en vigor cuando se graban por primera vez los datos en un volumen. Las actualizaciones de capacidad de escala realizadas en la clase de dispositivo no afectan a los volúmenes que ya tienen datos grabados hasta que el volumen vuelve a estar en estado reutilizable.

**Referencia relacionada:**

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior

---

Con IBM Spectrum Protect, puede utilizar los siguientes tipos de cifrados de unidad con unidades que sean 3592 generación 2 y posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

### Acerca de esta tarea

---

El parámetro DRIVEENCRYPTION del mandato DEFINE DEVCLASS especifica si se permite el cifrado de unidad para unidades que sean 3592 generación 2 y posterior. Utilice este parámetro para garantizar la compatibilidad de IBM Spectrum Protect con los ajustes de cifrado del hardware para volúmenes vacíos. No puede utilizar este parámetro para los volúmenes de agrupaciones de almacenamiento que estén llenos o se estén llenando.

- Para utilizar el método de aplicación en el que IBM Spectrum Protect genera y gestiona claves de cifrado, establezca el parámetro DRIVEENCRYPTION en ON. De esta forma, se habilita el cifrado de datos para volúmenes vacíos. Si el parámetro se establece en ON y el hardware está configurado para otro método de cifrado, las operaciones de copia de seguridad fallan.
- Para utilizar los métodos de cifrado de biblioteca o de sistema, establezca el parámetro en ALLOW. De esta manera, se especifica que IBM Spectrum Protect no es el gestor de claves del cifrado de unidad, aunque permitirá que el hardware cifre los datos del volumen mediante uno de los otros métodos. La especificación de este parámetro no implica un cifrado automático de los volúmenes. Los datos sólo se pueden cifrar especificando el parámetro ALLOW y configurando el hardware para que utilice uno de estos métodos.

El parámetro DRIVEENCRYPTION es opcional. El valor predeterminado es permitir los métodos de cifrado de biblioteca o de sistema.

### Procedimiento

---

En el siguiente ejemplo simplificado, se muestra cómo cifrar datos para volúmenes vacíos en una agrupación de almacenamiento utilizando IBM Spectrum Protect como gestor de claves:

1. Defina una biblioteca emitiendo el mandato DEFINE LIBRARY. Por ejemplo, emita el siguiente mandato:

```
define library 3584 libtype=SCSI
```

2. Defina una clase de dispositivos, 3592\_ENCRYPT emitiendo el mandato DEFINE DEVCLASS y especificando el valor ON para el parámetro DRIVEENCRYPTION. Por ejemplo, emita el siguiente mandato:

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```

3. Defina una agrupación de almacenamiento. Por ejemplo, emita el siguiente mandato:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

### Qué hacer a continuación

---

Para inhabilitar cualquier método de cifrado en los volúmenes nuevos, establezca el parámetro DRIVEENCRYPTION en OFF. Si el hardware está configurado para cifrar los datos mediante el método de Biblioteca o el de Sistema y DRIVEENCRYPTION está establecido en OFF, las operaciones de copia de seguridad fallarán.

## Configuración de la compartición de bibliotecas

---

Varios servidores de IBM Spectrum Protect pueden compartir dispositivos de almacenamiento por medio de una red de área de almacenamiento (SAN). Se debe configurar un servidor como gestor de biblioteca y los demás servidores como clientes de biblioteca.

### Antes de empezar

---

Asegúrese de que los sistemas cumplen los requisitos de licencia para la compartición de bibliotecas. Se requiere una autorización para IBM Spectrum Protect for SAN para cada servidor de IBM Spectrum Protect que se configura como cliente de biblioteca o como gestor de biblioteca en un entorno SAN.

### Acerca de esta tarea

---

En el caso de movimiento de datos sin LAN, los sistemas cliente de IBM Spectrum Protect pueden acceder directamente a los dispositivos de almacenamiento definidos en el servidor de IBM Spectrum Protect. Los agentes de almacenamiento instalados y configurados en los sistemas cliente llevan a cabo el traspaso de datos.

Para configurar la compartición de bibliotecas, debe definir un servidor de IBM Spectrum Protect como gestor de biblioteca para la configuración de la biblioteca compartida. A continuación, debe definir otros servidores de IBM Spectrum Protect como clientes de biblioteca que se comunican y solicitan recursos de almacenamiento al gestor de biblioteca. El servidor de gestor de biblioteca debe tener la misma versión o posterior que el servidor o servidores que están definidos como clientes de biblioteca.

## Procedimiento

---

Para completar los pasos siguientes para compartir los recursos de biblioteca en una SAN entre servidores de IBM Spectrum Protect, complete los pasos siguientes:

1. Configurar comunicaciones entre servidores.

Para compartir un dispositivo de almacenamiento en una SAN, defina los servidores entre sí mediante la función de definición cruzada. Cada servidor debe tener un nombre exclusivo.

2. Defina una biblioteca compartida y configure dispositivos de cinta en los sistemas servidor.

Utilice el procedimiento que se describe en Configuración de bibliotecas para su uso por parte de un servidor para definir una biblioteca para utilizarla en el entorno compartido. Modifique el procedimiento para definir la biblioteca como compartida, especificando el parámetro SHARED=YES para el mandato DEFINE LIBRARY.

3. Defina el servidor de gestor de bibliotecas.
4. Defina la biblioteca compartida en el servidor que es la biblioteca.
5. Desde el servidor de gestor de bibliotecas, defina las vías de acceso del cliente de biblioteca a cada unidad a la que puede acceder el cliente de biblioteca. El nombre de dispositivo debe reflejar la forma en que el sistema cliente de biblioteca reconoce el dispositivo de cinta. Se debe definir una vía de acceso desde el gestor de biblioteca a cada una de las unidades de cinta para que el cliente de biblioteca utilice la unidad.

Para evitar problemas, asegúrese de que todas las definiciones de vías de acceso a unidades definidas para el gestor de biblioteca estén definidas también para el cliente de biblioteca.



Por ejemplo, si el gestor de biblioteca define tres unidades de cinta, el cliente de biblioteca también debe definir tres unidades de cinta. Para limitar el número de unidades de cinta que un cliente de biblioteca puede utilizar a la vez, utilice el parámetro MOUNTLIMIT de la clase de dispositivo en el cliente de biblioteca.

6. Defina las clases de dispositivo para la biblioteca compartida.

El método preferido es hacer que los nombres de clase de dispositivo sean iguales en ambos servidores para evitar confusiones al definir varias clases de dispositivo con el mismo tipo de dispositivo y los mismos parámetros de biblioteca. Algunas operaciones, como la copia de seguridad de base de datos, utilizan el nombre de clase de dispositivo para identificar los datos para la copia de seguridad.

Los parámetros de clase de dispositivo especificados en el gestor de biblioteca prevalecen sobre los parámetros especificados para el cliente de biblioteca. Si los nombres de clase de dispositivo son distintos, el gestor de biblioteca utiliza los parámetros especificados en una clase de dispositivo que coincida con el tipo de dispositivo especificado para el cliente de biblioteca.


7. Defina una agrupación de almacenamiento para la biblioteca compartida.
8. Repita los pasos para configurar otro servidor como un cliente de biblioteca.


-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Compartir biblioteca para servidores AIX y Linux  
Para saber cómo configurar un entorno de compartición de bibliotecas SCSI para servidores que se ejecuten en sistemas AIX o Linux, revise el procedimiento de ejemplo.
- Ejemplo: compartición de bibliotecas para servidores Windows  
Para conocer cómo configurar un entorno de compartición de bibliotecas para servidores que funcionen en sistemas Windows, revise el procedimiento de ejemplo.

### Referencia relacionada:

 [DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

### Información relacionada:

 [DEFINE LIBRARY \(Definir una biblioteca\)](#)

 [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: Compartir biblioteca para servidores AIX y Linux

Para saber cómo configurar un entorno de compartición de bibliotecas SCSI para servidores que se ejecuten en sistemas AIX o Linux, revise el procedimiento de ejemplo.

### Acerca de esta tarea

En este ejemplo, se va a configurar un servidor de gestor de bibliotecas denominado ASTRO y un cliente de biblioteca denominado JUDY. Para ayudar a aclarar donde se realiza cada uno de los pasos, los mandatos van precedidos por el nombre de servidor desde el que se emite el mandato. La mayoría de los mandatos se emiten desde el cliente de biblioteca.

En las bibliotecas SCSI, puede definir la biblioteca especificando el parámetro `libtype=scsi`.

### Procedimiento

1. Para configurar ASTRO como el servidor de gestor de bibliotecas, defina una biblioteca de SCSI compartida denominada SANGROUP. Por ejemplo:

```
astro> define library sangroup libtype=scsi shared=yes
```

A continuación, complete el resto de los pasos como se describe en Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad para configurar la biblioteca.

Consejo: Puede utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca en un paso.

2. Defina ASTRO como servidor de gestor de bibliotecas emitiendo el mandato `DEFINE SERVER`.


```
judy> define server astro serverpassword=secret haddress=192.0.2.24
laddress=1777 crossdefine=yes
```

3. Defina la biblioteca compartida SANGROUP emitiendo el mandato `DEFINE LIBRARY`. Debe utilizar el nombre del servidor de gestor de bibliotecas en el parámetro `PRIMARYLIBMANAGER` y, después, utilizar `LIBTYPE=SHARED`.

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```

Asegúrese de que el nombre de biblioteca concuerde con el nombre de biblioteca en el gestor de biblioteca.


4. Defina las vías de acceso desde el gestor de biblioteca, ASTRO, a dos unidades de la biblioteca compartida emitiendo el mandato `DEFINE PATH`.

 Sistemas operativos AIX

```
astro> define path judy drivea srctype=server desttype=drive
library=sangroup device=/dev/rmt6
astro> define path judy driveb srctype=server desttype=drive
library=sangroup device=/dev/rmt7
```

 Sistemas operativos Linux

```
astro> define path judy drivea srctype=server desttype=drive
library=sangroup device=/dev/IBMtape6
astro> define path judy driveb srctype=server desttype=drive
library=sangroup device=/dev/IBMtape7
```

5. Defina todas las clases de dispositivo que están asociadas a la biblioteca compartida.  Sistemas operativos AIX

```
judy> define devclass tape library=sangroup devtype=lto
```

 Sistemas operativos Linux

```
judy> define devclass tape library=sangroup devtype=lto
```

Los siguientes parámetros de la definición de clase de dispositivo deben ser los mismos en el cliente de biblioteca y el gestor de biblioteca:

- o LIBRARY
- o DRIVEENCRYPTION
- o WORM
- o FORMAT

6. Defina una agrupación de almacenamiento denominada BACKTAPE que utilizará la biblioteca compartida. Emita el mandato `DEFINE STGPOOL`.


```
judy> define stgpool backtape tape maxscratch=50
```

## Qué hacer a continuación


---


Repita el procedimiento para definir más clientes de biblioteca para el gestor de biblioteca.


### Referencia relacionada:


 DEFINE DEVCLASS (Definir una clase de dispositivo)


### Información relacionada:

 DEFINE DRIVE (Definir una unidad en una biblioteca)

 DEFINE LIBRARY (Definir una biblioteca)

 DEFINE PATH (Definir una vía de acceso)

 DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

 Sistemas operativos Windows

## Ejemplo: compartición de bibliotecas para servidores Windows

---



Para conocer cómo configurar un entorno de compartición de bibliotecas para servidores que funcionen en sistemas Windows, revise el procedimiento de ejemplo.

### Acerca de esta tarea

---

En este ejemplo, se va a configurar un servidor de gestor de bibliotecas denominado ASTRO y un cliente de biblioteca denominado JUDY.

En las bibliotecas SCSI, puede definir la biblioteca especificando el parámetro `libtype=scsi`.

-  Sistemas operativos Windows Configuración del servidor gestor de bibliotecas  
Debe configurar el servidor gestor de bibliotecas con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN.
-  Sistemas operativos Windows Configuración de los servidores cliente de biblioteca  
Debe configurar uno o varios servidores de cliente de biblioteca con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN..

 Sistemas operativos Windows

## Configuración del servidor gestor de bibliotecas

---

Debe configurar el servidor gestor de bibliotecas con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN.

### Procedimiento

---

El procedimiento siguiente es un ejemplo de cómo configurar un servidor de IBM Spectrum Protect denominado ASTRO como gestor de bibliotecas.

1. Asegúrese de que el servidor gestor de bibliotecas se está ejecutando:
  - a. Inicie Windows Services Management Console (`services.msc`).
  - b. Seleccione el servicio. Por ejemplo, `TSM Server1`.
  - c. Si el servicio no está en ejecución, pulse con el botón derecho del ratón sobre el nombre del servicio y seleccione Iniciar.
2. Obtenga la información de biblioteca y de unidades del dispositivo de biblioteca compartida.
  - a. Ejecute el programa de utilidad `tsmdlst.exe`. Este programa de utilidad se encuentra en el directorio `\Program Files\Tivoli\TSM\server`.
3. Defina una biblioteca de tipo SCSI. Por ejemplo:

```
define library sangroup libtype=scsi shared=yes
```

En este ejemplo se utiliza el valor predeterminado para el número de serie de la biblioteca, es decir, el servidor obtiene el número de serie de la biblioteca en el momento en que se define la vía de acceso. Según las posibilidades de la biblioteca, es posible que el servidor no pueda detectar el número de serie automáticamente. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo.

4. Defina la vía de acceso desde el servidor hasta la biblioteca.

```
define path astro sangroup srctype=server desttype=library
device=lb0.0.0.2
```

Si no ha especificado el número de serie al definir la biblioteca, el servidor consulta ahora la biblioteca para obtener esta información. Si ha especificado el número de serie al definir la biblioteca, el servidor verifica la información definida y emite un mensaje si hay una discrepancia.

5. Defina las unidades en la biblioteca.

```
define drive sangroup drivea
define drive sangroup driveb
```

En este ejemplo se utiliza el valor predeterminado del número de serie de la unidad, que permite al servidor obtener el número de serie de la propia unidad en el momento en que se define la vía de acceso. Según las posibilidades de la unidad, es posible que el servidor no pueda detectar automáticamente el número de serie. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo.

En este ejemplo también se utiliza el valor predeterminado de la dirección de elemento de la unidad, que permite al servidor obtener el número de elemento de la propia unidad en el momento en que se define la vía de acceso.

La dirección de elemento es un número que indica la ubicación física de una unidad en una biblioteca automatizada. El servidor necesita la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Puede hacer que el servidor obtenga el número de elemento de la propia unidad en el momento en que se define la vía de acceso o puede especificar el número de elemento al definir la unidad.

Según las capacidades de la biblioteca, es posible que el servidor no pueda detectar automáticamente la dirección de elemento. En ese caso, deberá proporcionar la dirección de elemento al definir la unidad. Los números de elemento de muchas bibliotecas están disponibles en IBM® Support Portal for IBM Spectrum Protect.

6. Defina la vía de acceso desde el servidor a cada una de las unidades.

```
define path astro drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.2
```

Si no ha especificado el número de serie o la dirección de elemento al definir la unidad, el servidor consulta ahora la unidad o biblioteca para obtener esta información.

7. Defina al menos una clase de dispositivo.

```
define devclass tape devtype=dlt library=sangroup
```

8. Dé de alta el inventario de biblioteca. En el ejemplo siguiente se incorporan todos los volúmenes del inventario de la biblioteca como volúmenes reutilizables. El servidor utiliza el nombre que hay en la etiqueta de código de barras como nombre del volumen.

```
checkin libvolume sangroup search=yes status=scratch
checklabel=barcode
```

9. Defina una agrupación de almacenamiento para la biblioteca compartida con un máximo de 50 volúmenes reutilizables.


```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

**Referencia relacionada:**

- [CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)
- [DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

**Información relacionada:**

- [DEFINE DRIVE \(Definir una unidad en una biblioteca\)](#)
- [DEFINE LIBRARY \(Definir una biblioteca\)](#)
- [DEFINE PATH \(Definir una vía de acceso\)](#)
- [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)

 Sistemas operativos Windows

## Configuración de los servidores cliente de biblioteca

Debe configurar uno o varios servidores de cliente de biblioteca con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN..

## Antes de empezar

---

Asegúrese de que hay un servidor gestor de biblioteca definido.

## Acerca de esta tarea

---

Debe definir el servidor gestor de biblioteca. Utilice el procedimiento siguiente como ejemplo de cómo configurar un servidor de IBM Spectrum Protect denominado JUDY como cliente de biblioteca.

## Procedimiento

---

1. Asegúrese de que el servidor gestor de biblioteca se está ejecutando:
  - a. Inicie Windows Services Management Console (services.msc).
  - b. Seleccione el servicio. Por ejemplo, TSM Server1.
  - c. Si el servicio no está en ejecución, pulse con el botón derecho del ratón y seleccione Start.
2. Obtenga la información de biblioteca y de unidades del dispositivo de biblioteca compartida.
  - a. Ejecute el programa de utilidad `tsmdlst.exe`. Este programa de utilidad se encuentra en el directorio `\Program Files\Tivoli\TSM\server`.
3. Defina la biblioteca compartida, SANGROUP e identifique el gestor de biblioteca. Asegúrese de que el nombre de biblioteca concuerde con el nombre de biblioteca en el gestor de biblioteca.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Defina las vías de acceso desde el servidor cliente de biblioteca hasta cada unidades emitiendo mandatos en el cliente de administración:

```
define path judy drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.3
define path judy driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.3
```

5. Defina al menos una clase de dispositivo emitiendo mandatos desde el cliente de biblioteca:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10
library=sangroup
```

Establezca igual los parámetros para la clase de dispositivo en el cliente de biblioteca que en el gestor de biblioteca. También es recomendable que los nombres de clase de dispositivo sean iguales en ambos servidores, aunque no es obligatorio.

Los parámetros de clase de dispositivo especificados en el servidor gestor de biblioteca prevalecen sobre los especificados para el cliente de biblioteca. Esto es así independientemente de que los nombres de clase de dispositivo sean iguales en ambos servidores. Si los nombres de clase de dispositivo son distintos, el gestor de biblioteca utiliza los parámetros especificados en una clase de dispositivo que coincida con el tipo de dispositivo especificado para el cliente de biblioteca.

Si un cliente de biblioteca requiere un parámetro distinto del que se ha especificado en la clase de dispositivo del gestor de biblioteca (por ejemplo un límite de montaje distinto), siga los pasos siguientes:

- a. Cree una clase de dispositivo adicional en el servidor gestor de biblioteca. Especifique los valores de los parámetros que desea que utilice el cliente de biblioteca.
  - b. Cree una clase de dispositivo en el cliente de biblioteca con el mismo nombre y tipo de dispositivo que la nueva clase de dispositivo que ha creado en el servidor de biblioteca.
6. Defina la agrupación de almacenamiento, BACKTAPE, que utilizará la biblioteca compartida:

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

7. Repita este procedimiento para definir servidores adicionales como clientes de biblioteca.

### Referencia relacionada:

[DEFINE DEVCLASS](#) (Definir una clase de dispositivo)

### Información relacionada:

[DEFINE LIBRARY](#) (Definir una biblioteca)

[DEFINE PATH](#) (Definir una vía de acceso)

[DEFINE STGPOOL](#) (Definir un volumen en una agrupación de almacenamiento)

## Configuración de una jerarquía de agrupaciones de almacenamiento

---



Como parte del proceso de implementación, debe configurar una jerarquía de agrupación de almacenamiento. Configure al menos una agrupación de almacenamiento primario en el disco y una agrupación de almacenamiento primario en la cinta. Asegúrese de que los datos se migren de disco a cinta cada día.

## Antes de empezar

---

1. Asegúrese de revisar la información de Planificación de la jerarquía de agrupaciones de almacenamiento.
2. Asegúrese de que estén especificadas las reglas adecuadas, también conocidas como *políticas*, para realizar la copia de seguridad de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Asegúrese de que esté asignada una política a cada nodo. Para obtener instrucciones sobre cómo asignar una política cuando registra un nodo, consulte Registro de clientes.

## Procedimiento

---

Para configurar una jerarquía de agrupación de almacenamiento, complete los siguientes pasos:

1. Defina una agrupación de almacenamiento primario para el dispositivo de cinta emitiendo el mandato DEFINE STGPOOL.

Por ejemplo, defina una agrupación de almacenamiento primario, TAPE1, con una clase de dispositivo de LTO, y habilite la proximidad de grupo. Establezca el número máximo de volúmenes reutilizables que el servidor puede solicitar para esta agrupación de almacenamiento a 999. Emita el mandato siguiente:

```
define stgpool tape1 lto pooltype=primary collocate=group
maxscratch=999
```

2. Defina las unidades, vías de acceso y bibliotecas para la agrupación de almacenamiento primario en la cinta. Siga las instrucciones de Definición de dispositivos de cinta.
3. Defina una agrupación de almacenamiento primario para el dispositivo de disco emitiendo el mandato DEFINE STGPOOL.

Por ejemplo, defina una agrupación de almacenamiento, DISK1, con una clase de dispositivo de FILE. Asegúrese de que los datos se puedan migrar a la agrupación de almacenamiento de cinta, TAPE1, pero impida la migración automática especificando 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG. Impida la reclamación especificando 100 para el parámetro RECLAIM. Habilite la proximidad de nodo. Establezca el número máximo de volúmenes reutilizables que el servidor puede solicitar para esta agrupación de almacenamiento en 9999. Utilice el parámetro MIGPROCESS para especificar el número de procesos de migración. El valor del parámetro MIGPROCESS debe ser igual al número de unidades en la biblioteca menos el número de unidades que se reservan para operaciones de restauración. Emita el mandato siguiente:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Para obtener más información sobre cómo configurar la migración de disco a cinta, consulte Migración de agrupaciones de almacenamiento de disco.

## Qué hacer a continuación

---

Una jerarquía de agrupación de almacenamiento incluye solo agrupaciones de almacenamiento primario. Después de configurar la jerarquía de agrupación de almacenamiento, complete los pasos siguientes:

1. Cree una agrupación de almacenamiento de copias en un dispositivo de cinta. Para obtener instrucciones, consulte DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial).
2. Realice una copia de seguridad de la agrupación de almacenamiento primario en la agrupación de almacenamiento de copia utilizando el mandato BACKUP STGPOOL. Para obtener instrucciones, consulte BACKUP STGPOOL (Hacer copia de seguridad de los datos de la agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia).
3. Para asegurarse de que los datos se pueden recuperar en un desastre, configure un procedimiento para mover los volúmenes de cinta desde la agrupación de almacenamiento de copia a una ubicación fuera del local. Para obtener instrucciones, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.

### Referencia relacionada:

[CHECKIN LIBVOLUME](#) (Dar de alta un volumen de almacenamiento en una biblioteca)

### Información relacionada:

[DEFINE STGPOOL](#) (Definir un volumen en una agrupación de almacenamiento)

## Protección de aplicaciones y sistemas

---

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas.

- Adición de clientes  
Tras la configuración correcta del servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

## Configuración del movimiento de datos sin LAN


---

Puede configurar el cliente y el servidor de IBM Spectrum Protect de forma que el cliente, a través de un agente de almacenamiento, pueda mover datos directamente al almacenamiento en una SAN. Esta función, denominada movimiento de datos sin LAN, se proporciona en el producto IBM Spectrum Protect for SAN.

### Procedimiento

---

Para configurar el movimiento de datos sin LAN, complete los pasos siguientes. Para obtener información detallada al respecto, consulte la documentación de IBM Spectrum Protect for SAN.

1. Verifique la conexión de red.
2. Establezca comunicaciones entre el cliente, el agente de almacenamiento y el servidor.
3. Instale y configure el software en los sistemas cliente.
4. Configure dispositivos en el servidor a los que pueda acceder el agente de almacenamiento.
5. Configure políticas de IBM Spectrum Protect para el movimiento de datos sin LAN para el cliente.
6. Si utiliza almacenamiento FILE compartido, instale y configure IBM® TotalStorage SAN File System o IBM Spectrum Scale.  
 **Sistemas operativos Windows** Restricción: Si un volumen de IBM Spectrum Scale está formateado por un servidor AIX, el sistema Windows utiliza TCP/IP para transferir datos en lugar de la red de área de almacenamiento.
7. Defina vías de acceso desde el agente de almacenamiento hasta las unidades.
8. Inicie el agente de almacenamiento y verifique la configuración fuera de la LAN.

### Qué hacer a continuación

---

Para ajustar mejor el uso de los recursos de la LAN y la SAN, puede controlar la vía de acceso que siguen las transferencias de datos en el caso de los clientes que disponen de la función de movimiento de datos sin LAN. Controle la vía de acceso utilizando el mandato UPDATE NODE. Para cada cliente, puede seleccionar uno de los valores siguientes para las operaciones de lectura y grabación de datos. Especifique operaciones de lectura de datos utilizando el parámetro DATAREADPATH y operaciones de grabación utilizando el parámetro DATAWRITEPATH. El parámetro es opcional. El valor predeterminado es ANY.

LAN (solo vía de acceso LAN)

Especifique el valor de LAN si se cumple alguna de las siguientes condiciones:

- Si desea hacer copias de seguridad o restaurar una pequeña cantidad de datos.
- El cliente no tiene conectividad SAN.

LANFREE (solo vía de acceso sin LAN)

Especifique el valor LANFREE si el cliente y el servidor están en la misma SAN, y se cumple cualquiera de las siguientes condiciones:

- Si desea hacer copias de seguridad o restaurar una gran cantidad de datos.
- Desea descargar la carga de procesamiento del servidor en el cliente.
- Desea liberar la congestión de LAN.

ANY (cualquier vía de acceso disponible)

Se utiliza una vía de acceso fuera de la LAN si hay alguna disponible. Si no hay ninguna vía de acceso fuera de la LAN disponible, los datos se mueven mediante la LAN.

- Validación de la configuración fuera de la LAN  
Después de configurar un cliente de IBM Spectrum Protect para el movimiento de datos sin LAN, puede verificar la configuración y las definiciones de servidores con el mandato VALIDATE LANFREE.

## Métodos de cifrado de cinta

---

Decidir que método de cifrado utilizar depende de cómo quiera gestionar sus datos.

Es muy importante proteger los datos de cliente, especialmente si son datos confidenciales. Para garantizar la protección de los volúmenes dentro y fuera del local, está disponible la tecnología de cifrado de cinta de IBM.

La tecnología de cinta de IBM da soporte a distintos métodos de cifrado de unidades para los siguientes dispositivos:

- IBM 3592 generación 2 y generación 3
- IBM Linear Tape-Open (LTO) generación 4 y generación 5

Los métodos de cifrado de unidad que puede utilizar con IBM Spectrum Protect se configuran en el nivel del hardware. IBM Spectrum Protect no puede controlar ni cambiar qué método de cifrado se utiliza en la configuración del hardware. Si el hardware está configurado para el método Aplicación, IBM Spectrum Protect puede activar o desactivar el cifrado en función del valor de DRIVEENCRYPTION en la clase de dispositivo.

Para cifrar todos los datos de una determinada biblioteca lógica o para cifrar los datos en más que sólo volúmenes de agrupación de almacenamiento, utilice el método Sistema o Biblioteca. Si el gestor de claves de cifrado está configurado para compartir claves, los métodos Biblioteca y Sistema pueden compartir la clave de cifrado, lo que permite intercambiar los dos métodos. IBM Spectrum Protect no puede compartir o utilizar las claves de cifrado entre el método Aplicación y los métodos Sistema o Biblioteca del cifrado.

Tabla 1. Métodos de cifrado

| Método de cifrado      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cifrado de aplicación  | <p>Con el cifrado gestionado por aplicación, puede crear agrupaciones de almacenamiento dedicado que contengan solo volúmenes cifrados. De esta forma, podrá utilizar jerarquías de agrupaciones de almacenamiento y políticas para gestionar la forma de cifrar los datos.</p> <p>La aplicación, en este caso IBM Spectrum Protect, gestiona las claves de cifrado. IBM Spectrum Protect genera y almacena las claves en la base de datos del servidor. Los datos se cifran durante las operaciones de grabación, cuando la clave de cifrado se pasa del servidor a la unidad. Los datos se descifran para las operaciones de lectura.</p> <p>Para cifrar volúmenes de agrupación de almacenamiento y eliminar parte del procesamiento de cifrado en su sistema, habilite el método Aplicación. Utilice el cifrado gestionado por aplicación solo para volúmenes de agrupaciones de almacenamiento. Otros volúmenes, como las cintas de conjunto de copias de seguridad, los volúmenes de exportación y las copias de seguridad de bases de datos, no se cifran utilizando el método Aplicación.</p> <p>Requisito: Cuando se habilita el cifrado de aplicaciones, preste especial atención para proteger las copias de seguridad de las bases de datos porque las claves de cifrado que se utilizan para cifrar y descifrar datos se almacenan en la base de datos del servidor. Para restaurar los datos, debe tener la copia de seguridad de la base de datos correcta y las claves de cifrado correspondientes para acceder a la información. Asegúrese de hacer una copia de seguridad periódica de la base de datos y de salvaguardar las copias de seguridad para evitar su pérdida o sustracción. Cualquier persona que tenga acceso a la copia de seguridad y la base de datos y a las claves de cifrado tendrá acceso a sus datos.</p> |
| Cifrado de bibliotecas | <p>Con el cifrado gestionado por la biblioteca, puede controlar qué volúmenes se cifran utilizando sus números de serie. Puede especificar el rango o el conjunto de volúmenes que desea cifrar.</p> <p>Las claves de cifrado se gestionan mediante la biblioteca. Las claves se almacenan en un gestor de claves de cifrado y se proporcionan a la unidad. Si configura el hardware para utilizar el cifrado gestionado por la biblioteca, puede utilizar este método emitiendo el mandato DEFINE DEVCLASS y especificando el parámetro DRIVEENCRYPTION=ALLOW.</p> <p>Restricción: Solo determinadas bibliotecas de IBM dan soporte a IBM LTO-4 y cifrado posterior. Para obtener información detallada al respecto, consulte el apartado Configuración del cifrado de unidades de cinta.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



| Método de cifrado   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cifrado de sistemas | El cifrado gestionado por el sistema está disponible solo en el sistema operativo AIX®. El sistema operativo o el controlador de dispositivo gestiona las claves de cifrado que se proporcionan, y que se almacenan en un gestor de claves de cifrado. Si se configura el hardware para utilizar el cifrado de sistemas, puede utilizar este método emitiendo el mandato DEFINE DEVCLASS y especificando el parámetro DRIVEENCRYPTION=ALLOW. |

Para determinar si un volumen se cifra y qué método se ha utilizado, emita el mandato QUERY VOLUME y especifique el parámetro FORMAT=DETAILED.

- Configuración del cifrado de unidades de cinta  
Puede utilizar el cifrado de unidades para proteger cintas que contienen datos esenciales o confidenciales, por ejemplo, cintas que contengan información financiera confidencial. El cifrado de unidades puede ser útil al trasladar cintas del entorno de servidor de IBM Spectrum Protect a una ubicación externa o interna.

## Control de las operaciones de control de cintas

Las definiciones de clase de dispositivo para cintas incluyen parámetros que permiten controlar las operaciones de almacenamiento.

- Cómo rellena volúmenes IBM Spectrum Protect  
El mandato DEFINE DEVCLASS tiene un parámetro ESTCAPACITY opcional que indica la capacidad estimada de los volúmenes secuenciales asociados a la clase de dispositivo. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado utilizado.
- Especificar la capacidad estimada de los volúmenes de cinta  
IBM Spectrum Protect también utiliza la capacidad estimada para determinar cuándo empezar la reclamación de volúmenes de agrupación de almacenamiento.
- Especificación de formatos de grabación para soportes de cinta  
Puede especificar el formato de grabación utilizado por IBM Spectrum Protect para grabar datos en soportes de cinta. Si tiene previsto combinar generaciones de unidades, o distintos tipos de unidades, en una biblioteca, debe especificar un formato de registro para cada generación de unidad y cada tipo de unidad. De esta forma, el servidor puede diferenciar entre generaciones de unidades y tipos de unidad.
- Asociar objetos de biblioteca con clases de dispositivo  
Una biblioteca contiene las unidades que se pueden utilizar para montar un volumen. Sólo se puede asociar una biblioteca a una clase de dispositivo. Sin embargo, varias clases de dispositivo pueden hacer referencia a la misma biblioteca.
- Control de las operaciones de montaje de medios para dispositivos de cinta  
Utilizando definiciones de clases de dispositivo, puede controlar el número de volúmenes montados, el tiempo que un volumen está montado y el tiempo que el servidor de IBM Spectrum Protect espera a que haya una unidad disponible.
- Operaciones de preferencia  
El servidor puede preferir las operaciones de cliente o servidor en el caso de una operación de prioridad superior cuando se está utilizando un punto de montaje y no hay otros disponibles o cuando se necesita acceder a un volumen específico. Cuando se prefiere una operación, se cancela.
- Influencia de los cambios de dispositivo en la SAN  
El entorno SAN puede modificarse considerablemente debido a los cambios en el dispositivo o en el cableado. La naturaleza dinámica de la SAN puede hacer que las definiciones estáticas fallen o se vuelvan imprevisibles.
-  Sistemas operativos Windows Visualización de la información de dispositivos  
Puede visualizar información sobre los dispositivos conectados al servidor mediante el programa de utilidad de información de dispositivos (tsmdlst).
- Medios de cinta Grabar una vez leer varias  
Los soportes de cinta WORM (Grabar una vez leer varias) ayudan a evitar la supresión accidental o deliberada de datos fundamentales. Sin embargo, IBM Spectrum Protect impone ciertas restricciones y pautas a seguir cuando se utiliza el soporte de tipo Grabar una vez leer varias (WORM).
-  Sistemas operativos Windows Resolución de problemas con dispositivos  
Puede resolver errores que se producen cuando configura o usa dispositivos con IBM Spectrum Protect.

## Cómo rellena volúmenes IBM Spectrum Protect

El mandato DEFINE DEVCLASS tiene un parámetro ESTCAPACITY opcional que indica la capacidad estimada de los volúmenes secuenciales asociados a la clase de dispositivo. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado utilizado.

Si no se especifica el parámetro ESTCAPACITY, IBM Spectrum Protect utiliza un valor predeterminado en base al formato de grabación que se ha especificado para la clase de dispositivo utilizando el parámetro FORMAT.

Si especifica una capacidad estimada que excede la capacidad real del volumen de la clase de dispositivo, IBM Spectrum Protect actualiza la capacidad estimada del volumen cuando éste se llena. Cuando IBM Spectrum Protect alcanza el final del volumen, actualiza la capacidad según la cantidad de datos que se han grabado en el volumen.

Puede aceptar la capacidad estimada predeterminada de una clase de dispositivo determinada o especificar explícitamente una capacidad estimada. No es obligatorio que el valor de capacidad estimada sea exacto, pero resulta útil. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado que se utiliza. Puede que desee cambiar la capacidad estimada si se cumple una o las dos condiciones siguientes:

- La capacidad estimada predeterminada es inexacta debido a la compresión de datos.
- Tiene volúmenes de tamaño no estándar.

**Referencia relacionada:**

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Especificar la capacidad estimada de los volúmenes de cinta

---

IBM Spectrum Protect también utiliza la capacidad estimada para determinar cuándo empezar la reclamación de volúmenes de agrupación de almacenamiento.

### Acerca de esta tarea

---

Para las clases de dispositivo de cinta, los valores predeterminados seleccionados por el servidor dependen del formato de grabación que se utiliza para grabar datos en el volumen. Puede aceptar el valor predeterminado para un tipo de dispositivo o especificar un valor.

Para especificar la capacidad estimada para los volúmenes de cinta, utilice el parámetro ESTCAPACITY cuando defina la clase de dispositivo o actualice su definición.

**Referencia relacionada:**

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Especificación de formatos de grabación para soportes de cinta

---

Puede especificar el formato de grabación utilizado por IBM Spectrum Protect para grabar datos en soportes de cinta. Si tiene previsto combinar generaciones de unidades, o distintos tipos de unidades, en una biblioteca, debe especificar un formato de registro para cada generación de unidad y cada tipo de unidad. De esta forma, el servidor puede diferenciar entre generaciones de unidades y tipos de unidad.

### Acerca de esta tarea

---

Para especificar un formato de grabación, utilice el parámetro FORMAT al definir la clase de dispositivo o actualizar su definición.

Si todas las unidades asociadas con esa clase de dispositivo son idénticas, especifique FORMAT=DRIVE. El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen.

Si algunas unidades asociadas con una clase de dispositivo admiten un formato de densidad superior a otras, especifique un formato que sea compatible con todas las unidades.

Si las unidades de una biblioteca SCSI utilizan diferentes tecnologías de cinta (por ejemplo, DLT y LTO Ultrium), especifique un valor único para el parámetro FORMAT en cada definición de clase de dispositivo.

Para ver un ejemplo de configuración, consulte el apartado Ejemplo: Configurar una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad.

El formato de grabación que el servidor utiliza para un volumen se selecciona cuando se graban datos por primera vez en el volumen. La actualización del parámetro FORMAT no afecta a los medios que ya contienen datos hasta que dichos medios vuelven a grabarse desde el principio. Este proceso puede suceder tras reclamar o suprimir un volumen o una vez hayan caducado todos los datos del volumen.

**Referencia relacionada:**

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Asociar objetos de biblioteca con clases de dispositivo

---

Una biblioteca contiene las unidades que se pueden utilizar para montar un volumen. Sólo se puede asociar una biblioteca a una clase de dispositivo. Sin embargo, varias clases de dispositivo pueden hacer referencia a la misma biblioteca.

### Acerca de esta tarea

---

Para asociar una clase de dispositivo a una biblioteca, utilice el parámetro LIBRARY cuando defina una clase de dispositivo o actualice su definición.

**Referencia relacionada:**

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Control de las operaciones de montaje de medios para dispositivos de cinta

---

Utilizando definiciones de clases de dispositivo, puede controlar el número de volúmenes montados, el tiempo que un volumen está montado y el tiempo que el servidor de IBM Spectrum Protect espera a que haya una unidad disponible.

- Control del número de volúmenes montados simultáneamente  
Al establecer un límite de montaje para una clase de dispositivo, debe tener en cuenta el número de dispositivos de almacenamiento conectados al sistema. También debe tener en cuenta si va a utilizar la función de grabación simultánea, si asocia varias clases de dispositivo a una única biblioteca y el número de procesos que se ejecutan al mismo tiempo.
- Control de la cantidad de tiempo que un volumen permanece montado  
Puede controlar la cantidad de tiempo que un volumen permanece montado después de que haya tenido lugar la última actividad de E/S. Si hay un volumen que se utiliza con frecuencia, el rendimiento se puede mejorar estableciendo un período mayor de retención de montaje para evitar las operaciones innecesarias de montaje y desmontaje.
- Control de la cantidad de tiempo que un servidor espera una unidad  
Puede especificar el tiempo máximo, en minutos, que el servidor de IBM Spectrum Protect esperará hasta que haya una unidad disponible para la solicitud de montaje actual.

## Control del número de volúmenes montados simultáneamente

---

Al establecer un límite de montaje para una clase de dispositivo, debe tener en cuenta el número de dispositivos de almacenamiento conectados al sistema. También debe tener en cuenta si va a utilizar la función de grabación simultánea, si asocia varias clases de dispositivo a una única biblioteca y el número de procesos que se ejecutan al mismo tiempo.

### Acerca de esta tarea

---

Al seleccionar un límite de montaje para una clase de dispositivo, tenga en cuenta las siguientes cuestiones:

- ¿Cuántos dispositivos de almacenamiento están conectados al sistema?

No especifique un valor de límite de montaje superior al número de unidades asociadas disponibles que hay en la instalación. Si el servidor intenta montar tantos volúmenes como especifica el límite de montaje y no hay unidades disponibles para el volumen necesario, se produce un error y las sesiones de clientes pueden finalizar. (Esta restricción no se aplica cuando se especifica el parámetro DRIVES.)

Si comparte los recursos de la biblioteca en un SAN entre servidores IBM Spectrum Protect, debe limitar el número de unidades de cinta que un cliente de biblioteca puede utilizar a la vez. Para permitir que varios servidores de cliente de biblioteca utilicen una biblioteca de forma simultánea, especifique el parámetro MOUNTLIMIT al definir o actualizar la clase de dispositivo en el cliente de biblioteca. Para obtener más información sobre cómo configurar el uso compartido de la biblioteca, consulte Configuración de la compartición de bibliotecas.

- ¿Está utilizando la función de grabación simultánea para las agrupaciones de almacenamiento primarias, las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos?

Especifique un valor de límite de montaje que proporcione un número suficiente de puntos de montaje para dar soporte a la grabación simultánea de datos en la agrupación de almacenamiento primaria y en todas las agrupaciones de almacenamiento de copia asociadas y de datos activos.

- ¿Está asociando varias clases de dispositivo a una sola biblioteca?

Una clase de dispositivo asociada con una biblioteca puede utilizar cualquier unidad de la biblioteca que sea compatible con el tipo de dispositivo de esa clase. Puesto que se puede asociar más de una clase de dispositivo a una biblioteca, una misma unidad de la biblioteca podrá ser utilizada por más de una clase de dispositivo. IBM Spectrum Protect garantiza que dos operaciones no puedan utilizar la misma unidad simultáneamente utilizando dos clases de dispositivo diferentes.

- ¿Cuántos procesos de IBM Spectrum Protect quiere ejecutar al mismo tiempo, utilizando dispositivos en esta clase de dispositivo?

IBM Spectrum Protect cancela automáticamente algunos procesos para ejecutar otros procesos de prioridad superior. Si el servidor utiliza todas las unidades disponibles de una clase de dispositivo para realizar los procesos de prioridad superior, los procesos de prioridad inferior deben esperar hasta que queda disponible una unidad. Por ejemplo, IBM Spectrum Protect cancela el proceso para un cliente que realiza la copia de seguridad directamente en cinta si la unidad se necesita para un proceso de migración o de reclamación de cintas del servidor. IBM Spectrum Protect cancela un proceso de reclamación de cintas si la unidad se necesita para una operación de restauración de un cliente. Para obtener más información, consulte Operaciones de preferencia.

Si ocurre con frecuencia que unos procesos cancelan otros procesos, debe plantearse si puede hacer que haya más unidades disponibles para que IBM Spectrum Protect pueda utilizarlas. De lo contrario, revise la planificación de operaciones para reducir la posibilidad de colisiones al intentar obtener unidades.

Esta consideración también se aplica a la función de grabación simultánea. Para que la operación de grabación simultánea sea satisfactoria, debe haber suficientes unidades disponibles.

Para especificar el número máximo de volúmenes que pueden montarse simultáneamente, utilice el parámetro MOUNTLIMIT cuando defina la clase de dispositivo o actualice su definición.

**Referencia relacionada:**

[DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

**Información relacionada:**

[UPDATE DEVCLASS \(Actualizar una clase de dispositivo\)](#)

## Control de la cantidad de tiempo que un volumen permanece montado

---

Puede controlar la cantidad de tiempo que un volumen permanece montado después de que haya tenido lugar la última actividad de E/S. Si hay un volumen que se utiliza con frecuencia, el rendimiento se puede mejorar estableciendo un período mayor de retención de montaje para evitar las operaciones innecesarias de montaje y desmontaje.

### Acerca de esta tarea

---

Si las operaciones de montaje se manejan mediante actividades manuales asistidas por el operador, puede que desee especificar un período de retención de montaje más largo. Por ejemplo, si únicamente un operador proporciona soporte para toda la operación de un fin de semana, defina un período de retención de montaje elevado para que no se le solicite al operador que monte volúmenes a cada momento.

Para controlar la cantidad de tiempo que un volumen permanece montado, utilice el parámetro MOUNTRETENTION cuando defina la clase de dispositivo o actualice su definición. Por ejemplo, si el valor de retención de montaje es 60, y el volumen montado permanece desocupado durante 60 minutos, el servidor desmonta el volumen.

Mientras IBM Spectrum Protect tiene un volumen montado, la unidad está asignada a IBM Spectrum Protect y no se puede utilizar para nada más. Si necesita liberar la unidad para otros usos, puede cancelar las operaciones de IBM Spectrum Protect que utilizan la unidad y, a continuación, desmontar el volumen. Por ejemplo, puede cancelar las operaciones de migración o de copia de seguridad del servidor. Para obtener información sobre cómo cancelar los procesos y desmontar volúmenes, consulte Gestión de solicitudes del servidor para los volúmenes

**Referencia relacionada:**

[DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

**Información relacionada:**

[UPDATE DEVCLASS \(Actualizar una clase de dispositivo\)](#)

## Control de la cantidad de tiempo que un servidor espera una unidad

---

Puede especificar el tiempo máximo, en minutos, que el servidor de IBM Spectrum Protect esperará hasta que haya una unidad disponible para la solicitud de montaje actual.

### Acerca de esta tarea

---

Para controlar el tiempo de espera hasta que una unidad esté disponible para una solicitud de montaje, utilice el parámetro MOUNTWAIT cuando defina o actualice una clase de dispositivo.

**Referencia relacionada:**

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Operaciones de preferencia

---

El servidor puede preferir las operaciones de cliente o servidor en el caso de una operación de prioridad superior cuando se está utilizando un punto de montaje y no hay otros disponibles o cuando se necesita acceder a un volumen específico. Cuando se prefiere una operación, se cancela.

Puede utilizar el mandato QUERY MOUNT para ver el estado del volumen para el punto de montaje.

De forma predeterminada, la preferencia está habilitada en el servidor. Para inhabilitar la preferencia, especifique la opción NOPREEMPT en el archivo de opciones del servidor. Si especifica esta opción, el mandato BACKUP DB y los mandatos de exportación e importación son las únicas operaciones que pueden preferir otras operaciones.

- Preferencia del punto de montaje  
Si una operación de prioridad alta requiere un punto de montaje que está en una clase de dispositivo específica y todos los puntos de montaje de la clase de dispositivo están en uso, la operación de prioridad alta puede preferir un punto de montaje de una operación de prioridad más baja.
- Preferencia de acceso a un volumen  
Si una operación de prioridad alta requiere acceso a un volumen específico y ese volumen está en uso, la operación de prioridad alta puede adelantarse a la operación de prioridad más baja para ese volumen.

**Referencia relacionada:**

➔ BACKUP DB (Hacer copia de seguridad de la base de datos)

➔ QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)

## Preferencia del punto de montaje

---

Si una operación de prioridad alta requiere un punto de montaje que está en una clase de dispositivo específica y todos los puntos de montaje de la clase de dispositivo están en uso, la operación de prioridad alta puede preferir un punto de montaje de una operación de prioridad más baja.

Los puntos de montaje pueden adelantarse sólo cuando la clase de dispositivo de la operación preferente y la operación que se está adelantando es la misma.

Las siguientes operaciones de alta prioridad pueden tener preferencia respecto a otras operaciones para un punto de montaje.

- Operaciones de copia de seguridad de base de datos
- Operaciones de recuperación o restauración de HSM iniciadas por clientes
- Operaciones de restauración utilizando un transportador de datos remoto
- Operaciones de exportación
- Operaciones de importación
- Operaciones para generar conjuntos de copias de seguridad

Las operaciones siguientes no pueden anticiparse a otras operaciones ni otras pueden adelantarlas:

- Auditar un volumen
- Restaurar datos de una agrupación de copias o datos activos
- Preparar un archivo de plan de recuperación
- Almacenar datos con un transportador de datos remoto



Las operaciones siguientes se pueden anticipar y aparecen listadas por orden de prioridad, de mayor a menor prioridad. El servidor selecciona la operación de prioridad más baja para adelantarse, por ejemplo, a la identificación de duplicados.

- Replicar nodos
- Hacer copia de seguridad de datos en una agrupación de almacenamiento de copias
- Copiar datos activos a una agrupación de datos activos
- Traspasar datos a un volumen de agrupación de almacenamiento
- Migrar datos de un disco a un soporte secuencial
- Migrar datos de un soporte secuencial a otro soporte secuencial
- Operaciones de recuperación o restauración de HSM inicializadas por clientes
- Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial
- Identificar duplicados

## Preferencia de acceso a un volumen

---

Si una operación de prioridad alta requiere acceso a un volumen específico y ese volumen está en uso, la operación de prioridad alta puede adelantarse a la operación de prioridad más baja para ese volumen.

Por ejemplo, si una solicitud de restauración tiene que acceder a un volumen que está utilizando un proceso de reclamación y hay disponible una unidad, se cancelará el proceso de reclamación.

Las siguientes operaciones de alta prioridad pueden tener preferencia respecto a otras operaciones de acceso a un volumen específico:

- Operaciones de copia de seguridad de base de datos
- Operaciones de recuperación o restauración de HSM iniciadas por clientes
- Operaciones de restauración utilizando un transportador de datos remoto
- Operaciones de exportación
- Operaciones de importación
- Operaciones para generar conjuntos de copias de seguridad

Las operaciones siguientes no pueden anticiparse a otras operaciones ni otras pueden adelantarlas en el orden de preferencia:

- Auditar volumen
- Restaurar datos de una agrupación de copias o datos activos
- Preparar un plan de recuperación
- Almacenar datos con un transportador de datos remoto

Las operaciones siguientes se pueden anticipar y aparecen listadas por orden de prioridad, de mayor a menor prioridad. El servidor selecciona la operación de prioridad más baja para adelantarse, por ejemplo, a la identificación de duplicados.

- Replicar nodos
- Hacer copia de seguridad de datos en una agrupación de almacenamiento de copias
- Copiar datos activos a una agrupación de datos activos
- Traspasar datos a un volumen de agrupación de almacenamiento
- Migrar datos de un disco a un soporte secuencial
- Migrar datos de un soporte secuencial a otro soporte secuencial
- Realizar copia de seguridad, archivado o migración de datos HSM iniciada por el cliente
- Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial
- Identificar duplicados

## Influencia de los cambios de dispositivo en la SAN

---

El entorno SAN puede modificarse considerablemente debido a los cambios en el dispositivo o en el cableado. La naturaleza dinámica de la SAN puede hacer que las definiciones estáticas fallen o se vuelvan imprevisibles.

Los ID de los dispositivos que SAN ha asignado y que conocen el servidor y el agente de almacenamiento se pueden alterar debido a los restablecimientos del bus o a otros cambios de entorno. Por ejemplo, es posible que el servidor conozca un dispositivo X como *rmt0* (en AIX), en base a la especificación de la vía de acceso original al servidor y la configuración original de la LAN. Sin embargo, algunos sucesos de la SAN, por ejemplo, la adición de un nuevo dispositivo Y, hace que el dispositivo X se asigne a *rmt1*. Cuando el servidor intenta acceder al dispositivo X utilizando *rmt0*, falla el acceso o bien accede al dispositivo de destino equivocado. El servidor intenta recuperarse de cambios en dispositivos en la SAN utilizando números de serie de dispositivo para confirmar la identidad de los dispositivos con los que establece contacto.

Al definir una unidad o biblioteca, tiene la opción de especificar el número de serie de ese dispositivo. Si no especifica el número de serie al definir el dispositivo, el servidor obtiene el número de serie al definir la vía de acceso para el dispositivo. En cualquier caso, el

servidor tiene el número de serie de dispositivo en su base de datos y se puede utilizar para confirmar la identidad de un dispositivo para las operaciones.

Cuando el servidor utiliza unidades y bibliotecas en una SAN, el servidor intenta verificar que se utiliza el dispositivo correcto. El servidor establece contacto con el dispositivo utilizando el nombre de dispositivo en la vía de acceso que se ha definido para él. A continuación el servidor solicita el número de serie del dispositivo y lo compara con el que está almacenado en la base de datos del servidor para ese dispositivo.

Si el número de serie no coincide, el servidor inicia el proceso de detección en la SAN para intentar localizar el dispositivo con el número de serie coincidente. Si el servidor encuentra el dispositivo con el número de serie coincidente, corrige la definición de la vía de acceso en la base de datos del servidor actualizando el nombre de dispositivo de esa vía de acceso. El servidor emite un mensaje con información sobre el cambio efectuado en el dispositivo. El servidor no utiliza el dispositivo.

Para determinar si los cambios del dispositivo en la SAN afectan al servidor IBM Spectrum Protect, puede revisar el registro de actividad para obtener mensajes. Los siguientes mensajes están relacionados con números de serie:

- De ANR8952 a ANR8958
- De ANR8961 a ANR8968
- De ANR8974 a ANR8975

Restricción: Algunos dispositivos no tienen la posibilidad de informar de los números de serie a aplicaciones tales como el servidor de IBM Spectrum Protect. Si el servidor no puede obtener el número de serie de un dispositivo, el servidor no puede ayudar al sistema a recuperarse de un cambio de ubicación de dispositivo en la SAN.

 Sistemas operativos Windows

## Visualización de la información de dispositivos

---

Puede visualizar información sobre los dispositivos conectados al servidor mediante el programa de utilidad de información de dispositivos (tsmdlst).

### Antes de empezar

---

- Asegúrese de que la API HBA esté instalada. La API HBA es necesaria para ejecutar el programa de utilidad de información de dispositivos.
- Asegúrese de que el controlador de dispositivo de cinta esté instalado y configurado.

### Procedimiento

---

1. Desde un indicador de mandatos, vaya al subdirectorio `server` del directorio de instalación del servidor, por ejemplo, `C:\Program Files\Tivoli\TSM\server`.
2. Ejecute el archivo ejecutable `tsmdlst.exe`.

#### Referencia relacionada:

- [QUERY SAN \(consultar los dispositivos de SAN\)](#)
- [tsmdlst \(Visualizar la información sobre los dispositivos\)](#)

## Medios de cinta Grabar una vez leer varias

---

Los soportes de cinta WORM (Grabar una vez leer varias) ayudan a evitar la supresión accidental o deliberada de datos fundamentales. Sin embargo, IBM Spectrum Protect impone ciertas restricciones y pautas a seguir cuando se utiliza el soporte de tipo Grabar una vez leer varias (WORM).

Puede utilizar los siguientes tipos de medios WORM con IBM Spectrum Protect:

- IBM® 3592, todas las generaciones soportadas
- IBM LTO-3 y todas las generaciones soportadas
- HP LTO-3 y todas las generaciones soportadas
- Quantum LTO-3 y todas las generaciones soportadas
- Quantum SDLT 600, Quantum DLT V4 y Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 y AIT100

Sugerencias:

- Una agrupación de almacenamiento puede componerse de medios WORM o RW, pero no de ambos.

- Para evitar desperdiciar cinta después de una operación de restauración o importación, no utilice cintas WORM para operaciones de exportación o copia de seguridad de base de datos.
- Unidades preparadas para WORM  
Para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben estar habilitadas para WORM. Si se monta un cartucho WORM en una unidad de lectura/escritura (RW), el montaje dará error.
- Incorporación de medios WORM  
El tipo de los medios WORM determina si la etiqueta del medio debe ser leído durante la incorporación.
- Restricciones en los medios WORM  
No puede utilizar los medios WORM preetiquetados con la clase de dispositivo LTO ni ECARTRIDGE.
- Errores de montaje con medios WORM  
Si se cargan medios de cinta WORM en una unidad para un montaje de clase de dispositivo de lectura-grabación (RW), se producirá un error de montaje. De forma similar, si se cargan medios de cinta RW en una unidad para un montaje de clase de dispositivo WORM, el montaje fallará.
- Volver a etiquetar soportes WORM  
No puede volver a etiquetar un cartucho WORM si éste contiene datos. Esto es aplicable a cartuchos Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM e IBM 3592. La etiqueta de un volumen VolSafe sólo se puede sobregabar una vez y únicamente si el volumen no contiene datos utilizables, suprimidos o caducados.
- Eliminar volúmenes WORM privados de una biblioteca  
Si lleva a cabo alguna acción en un volumen WORM (por ejemplo, si suprime espacios de archivos) y el servidor no marca el volumen como lleno, el volumen vuelve al estado de reutilizable. Si un volumen WORM no se marca como lleno y se suprime de una agrupación de almacenamiento, el volumen permanecerá privado. Para suprimir un volumen WORM privado de una biblioteca, debe emitir el mandato CHECKOUT LIBVOLUME.
- Creación de volúmenes DLT WORM  
Los volúmenes DLT WORM se pueden convertir desde volúmenes de lectura-grabación (RW).
- Soporte para cintas 3592 WORM cortas y normales  
IBM Spectrum Protect admite cintas 3592 WORM cortas y normales. Para obtener los mejores resultados, defínalas en agrupaciones de almacenamiento distintas.
- Consultar a una clase de dispositivo el valor del parámetro WORM  
Puede determinar el valor del parámetro WORM en una clase de dispositivo utilizando el mandato QUERY DEVCLASS. La salida contiene un campo con la etiqueta WORM y un valor (YES o NO).

## Unidades preparadas para WORM

---

Para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben estar habilitadas para WORM. Si se monta un cartucho WORM en una unidad de lectura/escritura (RW), el montaje dará error.

No obstante, una unidad que admita WORM puede utilizarse como unidad RW si el parámetro WORM de la clase de dispositivo se establece en NO. Cualquier tipo de biblioteca puede tener tanto medios WORM como medios RW si *todas* las unidades admiten WORM. La única excepción a esta regla son las bibliotecas conectadas en red (NAS), en las que no pueden utilizarse medios de cintas WORM.

### Referencia relacionada:

[DEFINE DEVCLASS](#) (Definir una clase de dispositivo)

### Información relacionada:

[UPDATE DEVCLASS](#) (Actualizar una clase de dispositivo)

## Incorporación de medios WORM

---

El tipo de los medios WORM determina si la etiqueta del medio debe ser leído durante la incorporación.

Los cambiadores de biblioteca no pueden identificar la diferencia entre los medios de cinta de lectura/escritura (RW) normales y los siguientes tipos de medios de cinta WORM:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Para determinar el tipo de medio WORM utilizado, hay que cargar un volumen en una unidad. Por lo tanto, al dar de alta uno de estos tipos de volúmenes WORM, debe utilizar la opción CHECKLABEL=YES en el mandato CHECKIN LIBVOLUME.

Si dan soporte para los medios WORM, los cambiadores de biblioteca IBM® 3592 pueden detectar si un volumen es un medio WORM sin cargar el volumen en una unidad. No es necesario especificar CHECKLABEL=YES. Verifique con los proveedores de hardware que

sus bibliotecas y unidades 3592 proporcionan el soporte necesario.

**Referencia relacionada:**

[CHECKIN LIBVOLUME](#) (Dar de alta un volumen de almacenamiento en una biblioteca)

## Restricciones en los medios WORM

---

No puede utilizar los medios WORM preetiquetados con la clase de dispositivo LTO ni ECARTRIDGE.

No puede utilizar el soporte WORM con IBM Spectrum Protect especificado como gestor de claves de cifrado de unidad para las siguientes unidades:

- IBM® LTO-5, LTO-6, y posterior
- HP LTO-5, LTO-6, y posterior
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

## Errores de montaje con medios WORM

---

Si se cargan medios de cinta WORM en una unidad para un montaje de clase de dispositivo de lectura-grabación (RW), se producirá un error de montaje. De forma similar, si se cargan medios de cinta RW en una unidad para un montaje de clase de dispositivo WORM, el montaje fallará.

## Volver a etiquetar soportes WORM

---

No puede volver a etiquetar un cartucho WORM si éste contiene datos. Esto es aplicable a cartuchos Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM e IBM® 3592. La etiqueta de un volumen VolSafe sólo se puede sobregabar una vez y únicamente si el volumen no contiene datos utilizables, suprimidos o caducados.

Emita el mandato LABEL LIBVOLUME una sola vez para los volúmenes VolSafe. Puede proteger la etiqueta contra sobrescritura mediante la opción OVERWRITE=NO del mandato LABEL LIBVOLUME.

**Referencia relacionada:**

[LABEL LIBVOLUME](#) (Etiquetar un volumen de biblioteca)

## Eliminar volúmenes WORM privados de una biblioteca

---

Si lleva a cabo alguna acción en un volumen WORM (por ejemplo, si suprime espacios de archivos) y el servidor no marca el volumen como lleno, el volumen vuelve al estado de reutilizable. Si un volumen WORM no se marca como lleno y se suprime de una agrupación de almacenamiento, el volumen permanecerá privado. Para suprimir un volumen WORM privado de una biblioteca, debe emitir el mandato CHECKOUT LIBVOLUME.

**Referencia relacionada:**

[CHECKOUT LIBVOLUME](#) (Dar de baja un volumen de almacenamiento de una biblioteca)

## Creación de volúmenes DLT WORM

---

Los volúmenes DLT WORM se pueden convertir desde volúmenes de lectura-grabación (RW).

Si dispone de unidades SDLT-600, DLT-V4 o DLT-S4 y desea habilitarlas para soportes WORM, actualice las unidades utilizando el firmware V30 o posterior disponible de Quantum. También puede utilizar software DLTIce para convertir volúmenes RW sin formatear o volúmenes en blanco en volúmenes WORM.

En bibliotecas SCSI, el servidor de IBM Spectrum Protect crea volúmenes DLT WORM reutilizables de forma automática cuando el servidor no puede localizar ningún volumen WORM reutilizable en el inventario de una biblioteca. El servidor convierte los volúmenes reutilizables RW en blanco o sin formato disponibles o los volúmenes privados RW vacíos en volúmenes WORM reutilizables. El servidor también vuelve a grabar etiquetas sobre volúmenes WORM recién creados utilizando la información de etiqueta sobre los volúmenes RW existentes.

## Soporte para cintas 3592 WORM cortas y normales


---

IBM Spectrum Protect admite cintas 3592 WORM cortas y normales. Para obtener los mejores resultados, defínalas en agrupaciones de almacenamiento distintas.

## Consultar a una clase de dispositivo el valor del parámetro WORM

Puede determinar el valor del parámetro WORM en una clase de dispositivo utilizando el mandato QUERY DEVCLASS. La salida contiene un campo con la etiqueta WORM y un valor (YES o NO).

### Información relacionada:

 QUERY DEVCLASS (Visualizar información en una o más clases de dispositivo)

 Sistemas operativos Windows



## Resolución de problemas con dispositivos

Puede resolver errores que se producen cuando configura o usa dispositivos con IBM Spectrum Protect.

### Acerca de esta tarea

Utilice Tabla 1 para encontrar una solución a un problema relacionado con dispositivos.

Tabla 1. Resolución de problemas de dispositivos

| Síntoma                                        | Problema                                                                                                                           | Solución                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conflictos con otras aplicaciones.             | IBM Spectrum Protect requiere una red de área de almacenamiento para compartir dispositivos.                                       | Configure una red de área de almacenamiento.<br>Atención: Puede producirse una pérdida de datos si varios servidores de IBM Spectrum Protect utilizan el mismo dispositivo. Defina o utilice un dispositivo con un solo un servidor de IBM Spectrum Protect.<br> Sistemas operativos AIX<br> Sistemas operativos LinuxOtras aplicaciones pueden acceder a los dispositivos IBM Spectrum Protect, utilizando un controlador de cinta SCSI. |
| El etiquetado falla.                           | No es posible utilizar un dispositivo para etiquetar volúmenes mientras el servidor utiliza dicho dispositivo para otros procesos. | No puede sobrescribir los volúmenes existentes en una agrupación de almacenamiento.<br>Debe resolver cualquier problema de hardware antes de etiquetar un volumen.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                | Registro de licencia incorrecto o incompleto.                                                                                      | Registre la licencia del soporte de dispositivo que ha adquirido.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Conflictos entre controladores de dispositivo. | IBM Spectrum Protect emite mensajes sobre errores de E/S cuando define o utiliza un dispositivo de acceso secuencial.              | Los controladores de dispositivos de Windows y los controladores proporcionados por otras aplicaciones pueden interferir con el controlador de dispositivo de IBM Spectrum Protect si el controlador de IBM Spectrum Protect no se inicia primero. Para comprobar el orden en el que el sistema inicia los controladores de dispositivo, complete los pasos siguientes:<br><br><ol style="list-style-type: none"> <li>1. Pulse en Panel de control.</li> <li>2. Pulse en Dispositivos. Aparecerá una lista de los controladores de dispositivo y de sus tipos de arranque.</li> </ol>                               |

| Síntoma        | Problema                                                                                                                                                                                                                                                                                                                          | Solución |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Errores de E/S | Al intentar definir o utilizar un dispositivo de cinta, pueden producirse conflictos en el controlador de dispositivo. Los controladores de dispositivo de Windows y los controladores proporcionados por otras aplicaciones pueden interferir con el controlador de dispositivo de IBM Spectrum Protect si no se inicia primero. |          |

## Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

### Procedimiento

- Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
  - En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
  - En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
  - Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.  
Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.
- Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de cinta.

## Supervisión de una solución de cinta

Tras implementar una solución basada en cinta de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

### Acerca de esta tarea

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema.

### Procedimiento

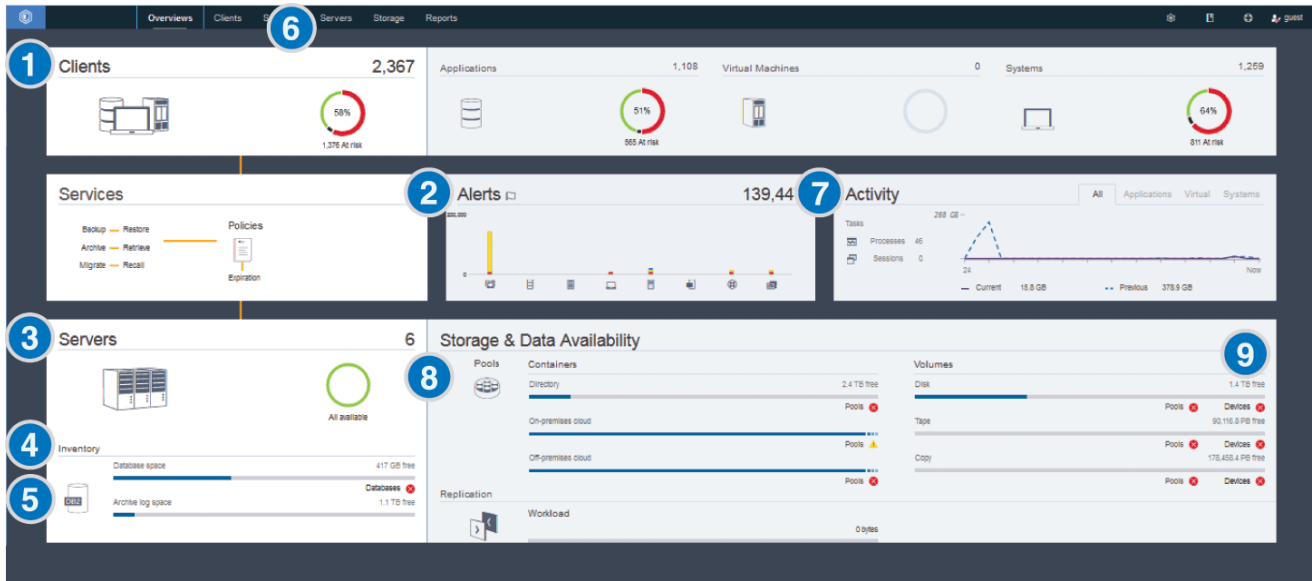
- Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación de supervisiones diarias.
- Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación de supervisiones periódicas.
- Verifique que su sistema cumple con los requisitos de licencia. Para obtener instrucciones, consulte Verificación de la conformidad de licencia.
- Opcional: Configure los informes de correo electrónico del estado del sistema. Para obtener instrucciones, consulte Seguimiento del estado del sistema mediante informes de correo electrónico


## Lista de comprobación de supervisión diaria

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.



Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.






La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.


Tabla 1. Tareas de supervisión diarias

| Tarea                                                                                                                                                  | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Procedimientos avanzados e información sobre solución de problemas                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1</b> Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p> | <p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Atención: Si el porcentaje En riesgo es superior al habitual, es posible que indique que se ha producido un ataque de ransomware. Un ataque de ransomware puede hacer que las operaciones de copia de seguridad fallen, poniendo a los clientes en una situación de riesgo. Por ejemplo, si el porcentaje de clientes en riesgo se encuentra habitualmente entre un 5% y un 10%, pero el porcentaje se incrementa a un 40% o 50%, investigue la causa. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Clientes, seleccione el cliente y pulse Detalles.</li> <li>2. Para diagnosticar un problema, pulse Diagnóstico.</li> </ol> | <p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p> |



| Tarea                                                                                                                                                                  | Procedimientos básicos                                                                                                                                                                                                                                                                                              | Procedimientos avanzados e información sobre solución de problemas                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>2</b> Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>                                                | <p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>                                                                                                                                                                                    | <p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Alertas.</li> <li>2. En la tabla Alertas, seleccione una alerta.</li> <li>3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.</li> </ol> |
| <p><b>3</b> Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p> | <ol style="list-style-type: none"> <li>1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible.</li> <li>2. Para ver información adicional, pulse el área Servidores.</li> <li>3. Seleccione un servidor en la tabla Servidores y pulse Detalles.</li> </ol> | <p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione un servidor y pulse Detalles.</li> <li>2. Para actualizar las propiedades de servidor, pulse Propiedades.</li> </ol>                                                                                    |





| Tarea                                                                                                                                                                                         | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Procedimientos avanzados e información sobre solución de problemas                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>4</b> Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p> | <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> <li>o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado.</li> <li>o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor.</li> <li>o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio.</li> <li>o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC.</li> <li>o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio.</li> </ul> </li> </ol> | <p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p> |

| Tarea                                                                                                                                                                                                                                     | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Procedimientos avanzados e información sobre solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>5</b> Verifique las operaciones de seguridad de la base de datos del servidor.</p>                                                                                                                                                  | <p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.</li> </ol>                                                                                                                                                                                 | <p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione una fila y pulse Detalles.</li> <li>2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad.</li> </ol> <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Servidores.</li> <li>2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad.</li> </ol> <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY DB: <pre>query db f=d</pre> </li> <li>3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.</li> </ol> |
| <p><b>6</b> Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p> | <p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse Servidores &gt; Mantenimiento.</li> <li>2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial.</li> <li>3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.</li> </ol> | <p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Tarea                                                                                                                                       | Procedimientos básicos                                                                                                                                                                                                                                                                                                  | Procedimientos avanzados e información sobre solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>7</b> Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p> | <ul style="list-style-type: none"> <li>• Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad.</li> <li>• Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.</li> </ul> | <ul style="list-style-type: none"> <li>• Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente. Atención: Si la cantidad de datos de copia de seguridad es significativamente superior a lo habitual, puede que indique un ataque de ransomware. Cuando un ransomware cifra datos, el sistema percibe que se están cambiando los datos, y realiza una copia de seguridad de los datos cambiados. Así, los volúmenes de copia de seguridad se vuelven más grandes. Para determinar qué clientes están afectados, pulse los separadores Aplicaciones, Virtual o Sistemas.</li> <li>• Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.</li> </ul> |

| Tarea                                                                                                                                     | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Procedimientos avanzados e información sobre solución de problemas                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>8</b> Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p> | <p>1. Si se indican problemas en el área Almacenamiento &amp; Disponibilidad de datos, pulse Agrupaciones para ver los detalles:</p> <ul style="list-style-type: none"> <li>○ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible.<br/>Atención: Si el estado es crítico, investigue la causa: <ul style="list-style-type: none"> <li>■ Si el índice de deduplicación de datos para una agrupación de almacenamiento cae significativamente, puede indicar un ataque de ransomware. Durante un ataque de ransomware, se cifran los datos y estos no podrán ser deduplicados. Para verificar el índice de deduplicación de datos, en la tabla Agrupaciones de almacenamiento, revise el valor de la columna % de ahorro.</li> <li>■ Si la agrupación de almacenamiento muestra inesperadamente un uso del 100%, esto puede indicar un ataque de ransomware. Para verificar la utilización, revise el valor de la columna Capacidad utilizada. Pase el cursor por encima de los valores para ver los porcentajes de espacio utilizado y libre.</li> </ul> </li> <li>○ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura.</li> </ul> <p>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</p> | <p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p> |

| Tarea                                                                                                             | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Procedimientos avanzados e información sobre solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>9</b> Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p> | <p>En el área Almacenamiento &amp; Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p> | <p>Es posible que los dispositivos de cinta tengan un estado de aviso o crítico si las unidades no están disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. También puede que un dispositivo de cinta tenga un estado crítico si la biblioteca está fuera de línea. Otras columnas de la tabla Dispositivos de cinta muestran el estado de la robótica, las unidades y las vías de acceso de la biblioteca.</p> <p>Para resolver problemas con unidades de cinta que tengan un estado crítico, sitúe la unidad fuera de línea si necesita utilizarla para otra actividad, como por ejemplo mantenimiento. Para poner una unidad fuera del sitio, complete los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Almacenamiento, seleccione Dispositivos de cinta.</li> <li>2. Para ver más información sobre una biblioteca de cintas, seleccione una fila y pulse Detalles.</li> <li>3. Para sacar una unidad fuera de línea, seleccione la unidad de cintas y pulse Fuera del sitio.</li> </ol> <p>Para las operaciones de copia de seguridad de cinta, compruebe que haya disponibles suficientes cintas reutilizables. Si no está seguro de si el número de cintas reutilizables es suficiente, abra el cuaderno de detalles para ver el uso de cintas y una estimación de la disponibilidad de cintas reutilizables. Para abrir el cuaderno de detalles, seleccione una biblioteca en la tabla y pulse Detalles.</p> |

## Lista de comprobación de supervisión periódica

Para asegurarse de que las operaciones se ejecutan correctamente, complete las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.








Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

| Tarea | Procedimientos básicos | Procedimientos avanzados y solución de problemas |
|-------|------------------------|--------------------------------------------------|
|-------|------------------------|--------------------------------------------------|

| Tarea                                        | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Procedimientos avanzados y solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Supervise el rendimiento del sistema.</p> | <p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Visión general, pulse Clientes. Busque el servidor asociado al cliente.</li> <li>2. Pulse Servidores. Seleccione el servidor y pulse Detalles.</li> <li>3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse Tareas completadas.</li> <li>4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Para obtener información sobre este mandato, consulte QUERY ACTLOG (Consultar las anotaciones de actividades).</li> <li>5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa.</li> </ol> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Visión general, pulse Clientes.</li> <li>2. Seleccione un cliente de archivado y copia de seguridad y pulse Detalles.</li> <li>3. Para recuperar registros de cliente, pulse Diagnóstico.</li> </ol> | <p>Limite el tiempo para las operaciones de copia de seguridad de cliente a 8 - 12 horas. Asegúrese de que las planificaciones de cliente no se solapen con las tareas de mantenimiento del servidor.</p> <p>Para obtener instrucciones sobre cómo reducir el tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte Resolución de problemas de rendimiento comunes del cliente.</p> <p>Busque cuellos de botella de rendimiento. Para obtener instrucciones, consulte Identificación de cuellos de botella de rendimiento.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte Rendimiento.</p> |

| Tarea                                                                                                                                                             | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Procedimientos avanzados y solución de problemas |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p> | <p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Visión general, pase el ratón sobre el icono de configuración y pulse en Creador de mandatos.</li> <li>2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory  query option devconfig</pre> </li> <li>3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.</li> </ol> <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p> |                                                  |

| Tarea                                                                                                 | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Procedimientos avanzados y solución de problemas |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <p>Determine si hay suficiente espacio disponible en el directorio para la instancia de servidor.</p> | <p>Verifique si hay al menos 50 GB de espacio libre disponible en el directorio para la instancia de servidor. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad.</li> </ul> <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux<br/>/home/tsminst1/tsminst1</li> <li>•  Sistemas operativos Windows<br/>C:\tsminst1</li> </ul> <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p> |                                                  |



| Tarea                                                  | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Procedimientos avanzados y solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Identifique la actividad de cliente inesperada.</p> | <p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Clientes.</li> <li>2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente.</li> <li>3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades.</li> <li>4. En el área Última sesión, visualice la fila Enviado a cliente.</li> </ol> | <p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p> <p>Revise de forma periódica la tabla de resumen de actividad SQL, que contiene estadísticas sobre las sesiones de cliente. Para comparar la actividad actual con la actividad previa, utilice una sentencia SQL SELECT. Si el nivel de actividad es significativamente diferente de la actividad anterior, puede que indique un ataque de ransomware.</p> <p>Revise de forma periódica el registro de actividad. Busque los mensajes de ANE que indican a cuántos archivos se les realizó copia de seguridad y fueron inspeccionados. Compare los índices de deduplicación de los datos actuales con los índices anteriores. Si se realizó una copia de seguridad a un número de archivos más alto de lo habitual, o el índice de deduplicación cae de forma inesperada a 0, puede indicar un ataque de ransomware.</p> |

| Tarea                                                                                     | Procedimientos básicos                                                                                                                                                                                                                                            | Procedimientos avanzados y solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p> | <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones.</li> <li>2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles.</li> </ol> | <p>Sugerencias:</p> <ul style="list-style-type: none"> <li>• Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> <li>3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>.</li> </ol> </li> <li>• Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>.</li> <li>• Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> </ol> </li> </ul> <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que hay disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> <li>• Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.</li> </ul> |

| Tarea                                                                                                                                                                                                                                                                                                      | Procedimientos básicos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Procedimientos avanzados y solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisar y mantener los dispositivos de cinta                                                                                                                                                                                                                                                            | <p>Puede supervisar su entorno para ver que no haya errores de hardware en las unidades de cinta ni en las bibliotecas de cintas. Para obtener instrucciones, consulte Supervisión de los mensajes de alerta de cinta sobre errores de hardware.</p> <p>Supervise la compatibilidad de los medios para prevenir errores en las unidades de cinta. Para obtener instrucciones, consulte Prevenir errores causados por la incompatibilidad de los medios.</p> <p>Supervise los mensajes de limpieza de las unidades de cinta. Para obtener instrucciones, consulte Operaciones con cartuchos limpiadores.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente no se solapen con las tareas de mantenimiento del servidor. Limite el tiempo para las operaciones de copia de seguridad de cliente a 8 - 12 horas.</p> | <p>En la página Centro de operaciones Descripción general, pulse Clientes &gt; Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>                                                                                                                                                                                                                                                                       | <p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones.</li> <li>2. Seleccione una planificación y pulse Detalles.</li> <li>3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila.</li> <li>4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado.</li> <li>5. Pulse Guardar.</li> </ol>                                                                                                                                                                                                                                                                                                  |
| <p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento no se solapen con las planificaciones de cliente.</p>                                                                                                        | <p>En la página Centro de operaciones Descripción general, pulse Servidores &gt; Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>                                                                                                                                                                                                                                                                                        | <p>El método preferido consiste en asegurarse de que cada tarea de mantenimiento se ejecute hasta el final antes de que se inicie la siguiente tarea de mantenimiento. Ejemplos de tareas de mantenimiento incluyen la caducidad de inventario, la copia de agrupaciones de almacenamiento, la reclamación de espacio y la copia de seguridad de base de datos. Consejo: Si una tarea de mantenimiento está en ejecución durante demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Visión general, pase el ratón sobre el icono de configuración y pulse en Creador de mandatos.</li> <li>2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener información sobre este mandato, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).</li> </ol> |

- Supervisión de los mensajes de alerta de cinta sobre errores de hardware  
Los dispositivos de cinta y biblioteca generan mensajes de alerta de cinta para informar de errores de hardware. Estos mensajes ayudan a determinar los problemas que no están relacionados con el servidor de IBM Spectrum Protect.
- Prevenir errores causados por la incompatibilidad de los medios  
Supervisando y resolviendo los problemas de compatibilidad de los medios, puede prevenir errores en una solución basada en cintas de IBM Spectrum Protect. Es posible que una unidad nueva tenga una capacidad limitada de utilizar formatos de medios

que sí están soportados en una versión anterior de la unidad. A menudo, una unidad nueva puede leer pero no grabar en formatos de medios anteriores.

- Operaciones con cartuchos limpiadores

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

## Supervisión de los mensajes de alerta de cinta sobre errores de hardware

---

Los dispositivos de cinta y biblioteca generan mensajes de alerta de cinta para informar de errores de hardware. Estos mensajes ayudan a determinar los problemas que no están relacionados con el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

---

Se crea una página de registro que se puede recuperar en cualquier momento o en un momento específico como, por ejemplo, cuando se desmonta una unidad.

Un mensaje de alerta de cinta puede tener uno de los siguientes niveles de gravedad:

- Informativo (por ejemplo, se ha intentado cargar un tipo de cartucho que no está permitido)
- Aviso (por ejemplo, se prevé un error de hardware)
- Crítico (por ejemplo, hay un problema con la cinta y los datos están en peligro)

De forma predeterminada, los mensajes de alerta de cinta están desactivados.

### Procedimiento

---

- Para habilitar los mensajes de alerta de cinta, emita el mandato SET TAPEALERTMSG y especifique el valor ON: `set tapealertmsg on`
- Para comprobar si los mensajes de alerta de cinta están habilitados, emita el mandato QUERY TAPEALERTMSG: `query tapealertmsg`

## Prevenir errores causados por la incompatibilidad de los medios

---

Supervisando y resolviendo los problemas de compatibilidad de los medios, puede prevenir errores en una solución basada en cintas de IBM Spectrum Protect. Es posible que una unidad nueva tenga una capacidad limitada de utilizar formatos de medios que sí están soportados en una versión anterior de la unidad. A menudo, una unidad nueva puede leer pero no grabar en formatos de medios anteriores.

### Acerca de esta tarea

---

De forma predeterminada, los volúmenes existentes con estado `FILLING` permanecen en ese estado después de una actualización de la unidad. En algunos casos, es posible que desee continuar utilizando una unidad anterior para llenar esos volúmenes. De este modo, puede conservar la posibilidad de lectura/escritura de los volúmenes existentes hasta que sean reclamados. Si opta por actualizar todas las unidades de una biblioteca, verifique que los formatos de los medios están soportados por el nuevo hardware. A menos que tenga pensado utilizar solo los medios más actuales con la nueva unidad, es necesario que sea consciente de los posibles problemas de compatibilidad. Para obtener instrucciones de migración, consulte el apartado Migración de datos a unidades actualizadas.

Para utilizar una nueva unidad con los medios en los que puede leer pero no grabar, emita el mandato `UPDATE VOLUME` para definir el acceso a esos volúmenes como de sólo lectura. De este modo se evitarán errores provocados por la incompatibilidad de lectura/escritura. Por ejemplo, una nueva unidad puede expulsar un medio que esté grabado en un formato que la unidad no admite al cargar el medio en la unidad. O puede que una nueva unidad dé error al emitir el primer mandato de grabar en un formato que la unidad no admite.

Cuando los datos del medio de sólo lectura caduquen y se reclame el volumen, sustitúyalo por un medio que sea totalmente compatible con la nueva unidad. Se pueden generar errores si una unidad nueva no puede calibrar correctamente un volumen grabado al utilizar un formato anterior. Para evitar este problema, asegúrese de que la unidad original esté funcionando correctamente y en los niveles de microcódigo actuales.

## Operaciones con cartuchos limpiadores

---

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

### Supervisión del proceso de limpieza

Si se ha incorporado un cartucho limpiador en una biblioteca y se tiene que limpiar una unidad, el servidor desmonta el volumen de datos y ejecuta la operación de limpieza. Si la operación de limpieza falla o se cancela, o si no hay ningún cartucho limpiador disponible, puede que no se dé cuenta de que la unidad necesita una limpieza. Supervise los mensajes sobre estos problemas de limpieza para asegurarse de que las unidades se limpian cuando es necesario. Si es necesario, emita el mandato CLEAN DRIVE para que el servidor intente la limpieza de nuevo, o cargue manualmente un cartucho limpiador en la unidad.

### Utilización de varios cartuchos limpiadores

El servidor utiliza un cartucho limpiador para el número de limpiezas que especifique al dar de alta el cartucho limpiador. Si incorpora dos o más cartuchos limpiadores, el servidor utilizará sólo uno de los cartuchos hasta alcanzar el número de limpiezas designado para ese cartucho. A continuación, el servidor utiliza el siguiente cartucho limpiador. Si incorpora dos o más cartuchos limpiadores y ejecuta simultáneamente dos o más mandatos CLEAN DRIVE, el servidor utilizará varios cartuchos al mismo tiempo y reducirá las limpiezas restantes en cada cartucho.

#### Referencia relacionada:

- ➔ AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ CLEAN DRIVE (Limpiar una unidad)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)

#### Información relacionada:

- ➔ QUERY LIBVOLUME (Consultar un volumen de biblioteca)

## Verificación de la conformidad de licencia

---

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

### Acerca de esta tarea

---

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

#### Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

#### Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

#### Licencia de PVU

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.

Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.



## Procedimiento

---

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

| Opción | Descripción |
|--------|-------------|
|--------|-------------|

| Opción                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Modelo frontal</b>       | <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p> |
| <b>Modelo suplementario</b> | <p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>                                                                                                                                                                                                                                                                                                                                                             |
| <b>Modelo de PVU</b>        | Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

### Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.
- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

### Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

### Procedimiento

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.  
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

## Resultados

---

Los informes habilitados se envían según los valores especificados.

## Qué hacer a continuación

---

El informe de operaciones general incluye un archivo adjunto. Para obtener información más detallada, expanda las secciones del archivo adjunto.

Si no puede ver la imagen de un informe, puede que esté utilizando un cliente de correo electrónico que convierte HTML a otro formato. Para obtener información sobre las restricciones, consulte la ayuda en línea Centro de operaciones.

## Gestión de operaciones para una solución de cinta

---

Utilice esta información para gestionar las operaciones para una implementación de cinta para un servidor IBM Spectrum Protect.

- **Gestión del Centro de operaciones**  
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.
- **Gestión de operaciones de cliente**  
Puede resolver errores de cliente, gestionar las actualizaciones de clientes y anular los nodos de cliente que ya no sean necesarios. Para liberar espacio de almacenamiento en el servidor, puede desactivar datos obsoletos almacenados por clientes de aplicación.
- **Gestión del almacenamiento de datos**  
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Gestión de dispositivos de cinta**  
Las operaciones rutinarias de cinta incluyen la preparación de volúmenes de cinta para su utilización, controlar cómo y cuándo se reutilizan los volúmenes y asegurarse de que hay suficientes volúmenes disponibles. También debe responder a las solicitudes de operador y gestionar bibliotecas, unidades, discos, vías de acceso y transportadores de datos.
- **Gestión de unidades de cinta**  
Puede consultar, actualizar y suprimir las unidades de cinta. También puede limpiar las unidades de cinta y configurar el cifrado de unidades de cinta y la validación de datos.
- **Protección del servidor IBM Spectrum Protect**  
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**  
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**  
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**  
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Preparación ante desastres y recuperación tras desastres mediante DRM**  
IBM Spectrum Protect proporciona una función de gestor recuperación tras desastre (DRM) para poder recuperar los datos del servidor y del cliente durante un siniestro.

## Gestión del Centro de operaciones

---

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.

## Acerca de esta tarea

---

Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect. Para obtener más información sobre la gestión del Centro de operaciones, consulte Gestión del Centro de operaciones.

## Gestión de operaciones de cliente

---

Puede resolver errores de cliente, gestionar las actualizaciones de clientes y anular los nodos de cliente que ya no sean necesarios. Para liberar espacio de almacenamiento en el servidor, puede desactivar datos obsoletos almacenados por clientes de aplicación.

### Acerca de esta tarea

---

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

Para obtener instrucciones sobre cómo añadir clientes, consulte Protección de aplicaciones y sistemas.

- **Evaluación de errores en registros de errores de cliente**  
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- **Detención y reinicio del aceptador de cliente**  
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- **Restablecimiento de contraseñas**  
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- **Gestión de actualizaciones del cliente**  
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- **Poner fuera de servicio un nodo cliente**  
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- **Desactivación de datos para liberar espacio de almacenamiento**  
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

## Evaluación de errores en registros de errores de cliente

---

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

### Antes de empezar

---

Opcionalmente, para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación Instalación del servicio de gestión de cliente.

### Procedimiento

---

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Detalles.
  3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
  4. Revise los mensajes de registro recuperados.Sugerencias:



- Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
- Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.

- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

## Detención y reinicio del aceptador de cliente

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

### Acerca de esta tarea

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

### Procedimiento

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
  - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```


Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:

- a. Pulse Inicio > Herramientas administrativas > Servicios.

- b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Iniciar y Aceptar.

**Referencia relacionada:**

 Resolución de problemas de planificación del cliente

## Restablecimiento de contraseñas

---

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

### Procedimiento

---

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nodo cliente y *nueva\_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como generar en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva\_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:

1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nombre del nodo y *nueva\_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como generar en el archivo de opciones del cliente.

## Gestión de actualizaciones del cliente

---

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

### Antes de empezar

---

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

## Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

| Software                                                        | Enlace a instrucciones                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cliente de copia de seguridad/archivado de IBM Spectrum Protect | <ul style="list-style-type: none"> <li>• Planificación de actualizaciones del cliente</li> </ul>                                                                                                                                                                                                                                                                     |
| IBM Spectrum Protect Snapshot                                   | <ul style="list-style-type: none"> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li> </ul>                                                            |
| IBM Spectrum Protect for Databases                              | <ul style="list-style-type: none"> <li>• Actualización de Data Protection for SQL Server</li> <li>• Instalación de Data Protection for Oracle</li> <li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>                                                                           |
| IBM Spectrum Protect for Enterprise Resource Planning           | <ul style="list-style-type: none"> <li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>                                                                                    |
| IBM Spectrum Protect for Mail                                   | <ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> <li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect for Virtual Environments                   | <ul style="list-style-type: none"> <li>• Instalación y actualización de Data Protection for VMware</li> <li>• Instalación de Data Protection for Microsoft Hyper-V</li> </ul>                                                                                                                                                                                        |

## Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

### Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot

- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

## Procedimiento

---

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
  1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
  2. Pulse Más > Poner fuera de servicio.
- Para que un nodo cliente quede fuera de servicio utilizando un mandato administrativo, realice una de las siguientes acciones:
  - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Qué hacer a continuación

---

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
  - o Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
  - o Un valor null especifica que el nodo no está fuera de servicio.
  - o Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- o Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

| Proceso proceso | Descripción proceso | Estado proceso                                                                                   |
|-----------------|---------------------|--------------------------------------------------------------------------------------------------|
| 3               | DECOMMISSION NODE   | Número de objetos de copia de seguridad desactivados para el nodo NODE1: 8 objetos desactivados. |

- o Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- o Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

**Referencia relacionada:**

- ➔ DECOMMISSION NODE (Poner fuera de servicio un nodo de cliente)
- ➔ DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

## Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

### Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

### Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.  
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

**Referencia relacionada:**

- ➔ DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

## Gestión del almacenamiento de datos

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Gestión de la capacidad de inventario  
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

- Ajuste de actividades planificadas  
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.
- Optimización de operaciones habilitando la función de proximidad de los archivos de cliente  
La proximidad de los archivos de cliente reduce el número de montajes de volúmenes necesarios cuando los usuarios restauran o recuperan muchos archivos de una agrupación de almacenamiento. Este modo de proximidad reduce la cantidad de tiempo necesario para estas operaciones.

**Referencia relacionada:**

➔ Tipos de agrupación de almacenamiento

## Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

### Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

### Procedimiento

- Para aumentar el espacio de disco para la base de datos, complete los pasos siguientes:
  - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
  - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.  
Sugerencias:
    - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
    - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
  - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
  - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.
- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, consulte la información en nota técnica 1683633. Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.
- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

|                                         |                                                                                                                          |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Valor de la opción ACTIVELOGSize</b> | <b>Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize</b> |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|

| Valor de la opción<br><b>ACTIVELOGSize</b> | Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de <b>ACTIVELOGSize</b> |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 16 GB - 128 GB                             | 5120 MB                                                                                                                  |
| 129 GB - 256 GB                            | 10240 MB                                                                                                                 |
| 257 GB - 512 GB                            | 20480 MB                                                                                                                 |

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activeologsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
  5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la compresión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la compresión del registro de archivado de forma inmediata sin detener el servidor.

#### Referencia relacionada:

- [ACTIVELOGSIZE](#), opción de servidor
- [EXTEND DBSPACE](#) (Incrementar el espacio para la base de datos)
- [SETOPT](#) (Establecer una opción de servidor para actualización dinámica)

## Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

### Procedimiento

1. Supervise el rendimiento de sistema de forma periódica para asegurarse de que las tareas de copia de seguridad y mantenimiento se completan correctamente. Para obtener más información sobre supervisión, consulte Supervisión de una solución de cinta.
2. Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, tal vez tenga que revisar la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
  - o El número de clientes aumenta.
  - o La cantidad de datos de los que se hace copia de seguridad aumenta.
  - o La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución tiene problemas de rendimiento. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
  - b. Pulse Detalles.
  - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos.
Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.
4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
  - a. Copia de seguridad de la base de datos
  - b. Ejecutar la caducidad para eliminar las copias de seguridad de cliente y las copias de archivo de archivado del almacenamiento de servidor.

#### Conceptos relacionados:

- [Rendimiento](#)

#### Tareas relacionadas:

## Optimización de operaciones habilitando la función de proximidad de los archivos de cliente

La proximidad de los archivos de cliente reduce el número de montajes de volúmenes necesarios cuando los usuarios restauran o recuperan muchos archivos de una agrupación de almacenamiento. Este modo de proximidad reduce la cantidad de tiempo necesario para estas operaciones.

### Acerca de esta tarea

Con la función de proximidad activada, el servidor intenta conservar todos los archivos en un mínimo de volúmenes de almacenamiento de acceso secuencial. Estos archivos pueden pertenecer a un único nodo de cliente, un grupo de nodos de cliente, un espacio de archivo cliente o a un grupo de espacios de archivo. Puede establecer la función de proximidad para cada agrupación de almacenamiento de acceso secuencial al definir o actualizar la agrupación.

Figura 1 muestra un ejemplo de proximidad por nodo cliente con tres clientes, cada uno con un volumen independiente que contiene los datos del cliente.

Figura 1. Ejemplo de proximidad habilitada por nodo



La Figura 2 muestra un ejemplo de la función de proximidad por grupo de nodos cliente. Se definen tres grupos, y los datos para cada grupo se almacenan en volúmenes independientes.

Figura 2. Ejemplo de proximidad habilitada por asignación de nodos

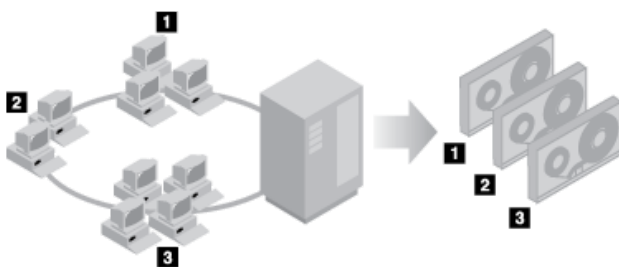
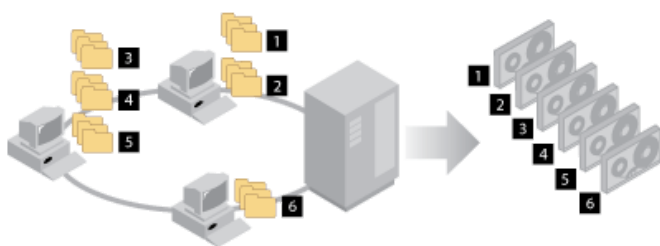


Figura 3 muestra un ejemplo de proximidad por grupo de espacio de archivos. Se definen seis grupos. Cada grupo contiene datos de los espacios de archivos que pertenecen a un único nodo. Los datos para cada grupo se almacenan en un volumen independiente.

Figura 3. Ejemplo de proximidad habilitada por el grupo de asignación del espacio de archivos

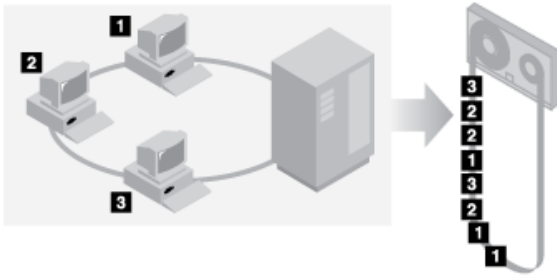


Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen antes de seleccionar un nuevo volumen. Este proceso mejora el uso de volúmenes individuales y los archivos de usuario se pueden distribuir en



muchos volúmenes. Figura 4 muestra un ejemplo de proximidad que está inhabilitada, con tres clientes que comparten el espacio en un único volumen.

Figura 4. Ejemplo de función de proximidad inhabilitada



Con la proximidad inhabilitada, es posible que se requieran más operaciones de montaje de medios para montar volúmenes cuando los usuarios restauren o recuperen muchos archivos.

La proximidad por grupo es el valor predeterminado del sistema IBM Spectrum Protect para agrupaciones de almacenamiento de acceso secuencial. El valor predeterminado para las agrupaciones de almacenamiento de copias es no proximidad.

- Efectos de la proximidad en las operaciones  
El efecto de la proximidad en los recursos y el rendimiento del sistema depende del tipo de operación que se realice.
- Selección de volúmenes con proximidad habilitada  
La selección del volumen depende de si la proximidad es por grupo, nodo o espacio de archivo.
- Selección de volúmenes con proximidad inhabilitada  
Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen de almacenamiento antes de acceder a otro volumen.
- Valores de proximidad  
Una vez definida una agrupación de almacenamiento, se puede cambiar el valor de la función de proximidad actualizando la agrupación de almacenamiento. La modificación de la agrupación con respecto a la función de proximidad no afecta a los archivos que ya están almacenados en la agrupación.
- Proximidad de agrupaciones de almacenamiento de copias  
En relación con la utilización de la función de proximidad en las agrupaciones de almacenamiento de copia, existen varios aspectos que debe tener en cuenta. La proximidad de agrupaciones de almacenamiento de copia, especialmente por nodo o espacio de archivo, implica más volúmenes parcialmente llenos y actividad de reclamación fuera del local potencialmente innecesaria.
- Planificación y activación de la función de proximidad  
Entender los efectos de la función de proximidad puede ayudar a reducir el número de montajes de medios, aprovechar mejor el espacio en volúmenes secuenciales y mejorar la eficacia de las operaciones de servidor.

## Efectos de la proximidad en las operaciones

El efecto de la proximidad en los recursos y el rendimiento del sistema depende del tipo de operación que se realice.

En la Tabla 1 se resume la incidencia de la proximidad en las operaciones.

Tabla 1. Efecto de la proximidad en las operaciones

| Operación                                                         | Proximidad habilitada                                                 | Proximidad inhabilitada                |
|-------------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------|
| Copia de seguridad, archivado o migración de archivos de clientes | Más montajes de medios para la función de proximidad de los archivos. | Se requieren menos montajes de medios. |

| <b>Operación</b>                                | <b>Proximidad habilitada</b>                                                                                                                                                                                                                                                                                                                                                                                      | <b>Proximidad inhabilitada</b>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restauración o recuperación de archivos cliente | Se pueden restaurar o recuperar numerosos archivos más rápidamente debido a que están situados en menos volúmenes.                                                                                                                                                                                                                                                                                                | Pueden necesitarse varios montajes de medios para un único usuario debido a que los archivos pueden estar distribuidos en varios volúmenes.<br><br>Pueden almacenarse archivos de más de un usuario en el mismo volumen de almacenamiento de acceso secuencial. Por ejemplo, si dos usuarios intentan recuperar un archivo que reside en el mismo volumen, el segundo usuario se verá obligado a esperar hasta que se hayan recuperado los archivos del primer usuario. |
| Almacenamiento de datos en cinta                | El servidor intenta utilizar todos los volúmenes de cinta disponibles para separar los archivos de usuario antes de utilizar todo el espacio disponible en cada volumen de cinta.                                                                                                                                                                                                                                 | El servidor intenta utilizar todo el espacio disponible en cada volumen de cinta antes de que el servidor utilice otro volumen de cinta.                                                                                                                                                                                                                                                                                                                                |
| Operaciones de montaje de medios                | Se requieren más operaciones de montaje cuando se realizan copias de seguridad, se archivan o se migran los archivos de usuario desde nodos de cliente directamente a volúmenes de acceso secuencial.<br><br>Se requieren más operaciones de montaje durante la reclamación y la migración de agrupaciones de almacenamiento.<br><br>Se gestionan más volúmenes porque los volúmenes no se utilizan por completo. | Se necesitan más operaciones de montaje durante la restauración y la recuperación de los archivos cliente.                                                                                                                                                                                                                                                                                                                                                              |
| Generación de conjuntos de copias de seguridad  | Se dedica menos tiempo a buscar entradas de bases de datos, y se necesitan menos operaciones de montaje.                                                                                                                                                                                                                                                                                                          | Se dedica más tiempo a buscar entradas de bases de datos, y se necesitan menos operaciones de montaje.                                                                                                                                                                                                                                                                                                                                                                  |

Cuando se habilita la proximidad para un grupo, un único nodo de cliente o espacio de archivos, un proceso de servidor mueve o copia todos los datos que pertenecen al grupo, el nodo o el espacio de archivos. Por ejemplo, si los datos se aproximan por grupo, todos los datos de todos los nodos que pertenecen al mismo grupo de proximidad se migran en el mismo proceso.

Cuando se aproximan datos, el servidor de IBM Spectrum Protect intentará mantener juntos los archivos en un número mínimo de volúmenes de almacenamiento de acceso secuencial. No obstante, cuando el servidor realice la copia de seguridad de datos a volúmenes en una agrupación de almacenamiento de acceso secuencial, el proceso de copia de seguridad tendrá prioridad sobre los valores de proximidad. Como resultado, el servidor completa la operación de copia de seguridad, pero es posible que no pueda aproximar los datos.

Por ejemplo, supongamos que está aproximando por nodo y que especifica que un nodo puede emplear dos puntos de montaje en el servidor. Supongamos también que los datos cuya copia de seguridad se está realizando desde un nodo, puedan caber fácilmente en un volumen de cinta. Durante la copia de seguridad, el servidor puede montar dos volúmenes de cinta y los datos del nodo se pueden distribuir en dos cintas, en vez de distribuirse en una sola. Si habilita la proximidad, las siguientes operaciones de servidor utilizan un proceso de servidor:

- Mover datos desde volúmenes de acceso aleatorio y de acceso secuencial
- Mover datos de nodo desde volúmenes de acceso secuencial
- Realizar copia de seguridad de una agrupación de almacenamiento de acceso aleatorio o de acceso secuencial.
- Restaurar una agrupación de almacenamiento de acceso secuencial.
- Reclamar espacio en una agrupación de almacenamiento de acceso secuencial o volúmenes fuera del local
- Migrar datos desde una agrupación de almacenamiento de acceso aleatorio

Si migra datos desde una agrupación de almacenamiento de disco de discos de acceso aleatorio a una agrupación de almacenamiento de acceso secuencial, y la proximidad es por nodo o espacio de archivos, los nodos o espacios de archivo se seleccionan automáticamente para la migración en función de la cantidad de datos que se migrarán. El nodo o el espacio de archivos con más cantidad de datos se migra en primer lugar. Si la proximidad es por grupo, todos los nodos de la agrupación de almacenamiento se evalúan en primer lugar para determinar qué nodo tiene más datos. El nodo con más datos se migra el primero junto con todos los

datos de todos los nodos pertenecientes a ese grupo de proximidad. Este proceso se realiza, independientemente de cuántos datos se almacenen en los espacios de archivo de los nodos y de si se ha alcanzado el umbral de migración inferior.

Sin embargo, si migra los datos de proximidad desde una agrupación de almacenamiento de acceso secuencial a otra agrupación de almacenamiento de acceso secuencial, el servidor ordena los volúmenes en función de la fecha en la que se accedió al volumen por última vez. El volumen con la fecha de acceso más reciente se migra primero, y el volumen con la última fecha de acceso se migra el último.

Un motivo para realizar la proximidad por grupo es que los nodos cliente individuales no suelen disponer de datos suficientes para llenar volúmenes de cinta de gran capacidad. La proximidad de datos por grupos de nodos puede reducir la capacidad de cinta no utilizada colocando más datos de proximidad en cintas individuales. Además, la proximidad de datos por grupos de espacios de archivos reduce la cinta no utilizada en mayor medida.

Los datos que pertenecen a todos los nodos del mismo grupo de proximidad se migran en el mismo proceso. Por tanto, la proximidad por grupo puede reducir el número de veces que se debe montar un volumen que se va a migrar. La proximidad por grupo también puede minimizar la exploración de bases de datos así como los pases de cinta durante la transferencia de datos de una agrupación de almacenamiento de acceso secuencial a otra.

## Selección de volúmenes con proximidad habilitada

La selección del volumen depende de si la proximidad es por grupo, nodo o espacio de archivo.

La Tabla 1 muestra la forma en que el servidor de IBM Spectrum Protect seleccione el primer volumen cuando la función de proximidad está activada para una agrupación de almacenamiento en el nodo de cliente, el grupo de proximidad y el nivel de espacio de archivos.

Tabla 1. Cómo selecciona volúmenes el servidor si la proximidad está activada

| Orden de selección de volúmenes | Cuando la proximidad es por grupo                                                                       | Cuando la proximidad es por nodo                                                                        | Cuando la proximidad es por espacio de archivos                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1                               | Un volumen que ya contiene archivos del grupo de proximidad al cual pertenece el cliente                | Un volumen que ya contiene archivos del mismo nodo cliente                                              | Un volumen que ya contiene archivos del mismo espacio de archivos de dicho nodo de cliente              |
| 2                               | Un volumen predefinido vacío                                                                            | Un volumen predefinido vacío                                                                            | Un volumen predefinido vacío                                                                            |
| 3                               | Un volumen reutilizable vacío                                                                           | Un volumen reutilizable vacío                                                                           | Un volumen reutilizable vacío                                                                           |
| 4                               | El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos | El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos | Un volumen que ya contiene archivos del mismo nodo de cliente                                           |
| 5                               | No aplicable                                                                                            | No aplicable                                                                                            | El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos |

Si el usuario debe continuar almacenando datos en un segundo volumen, utiliza la siguiente selección para adquirir más espacio:

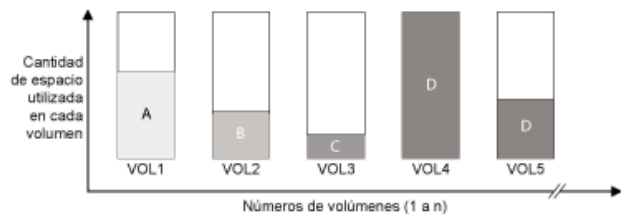
1. Un volumen predefinido vacío
2. Un volumen reutilizable vacío
3. El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos
4. Cualquier volumen disponible de la agrupación de almacenamiento

Cuando la proximidad es por nodo de cliente o por espacio de archivos, el servidor intenta proporcionar el mejor uso de los volúmenes individuales y minimizar la mezcla de archivos procedentes de distintos clientes o espacios de archivos en los volúmenes. Esta configuración está representada en Figura 1, que muestra que la selección de volúmenes es *horizontal*, donde se utilizan todos los volúmenes disponibles antes de utilizar todo el espacio disponible de cada volumen que se utiliza. A, B, C y D representan archivos de cuatro nodos cliente distintos.

Sugerencias:

1. Si la proximidad es por nodo y el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos.
2. Si la proximidad es por espacio de archivos y un nodo tiene varios espacios de archivos, el servidor intentará aproximar los datos para los distintos espacios de archivos en distintos volúmenes.

Figura 1. Utilización de todos los volúmenes de almacenamiento de acceso secuencial disponibles con la proximidad habilitada a nivel de espacio de archivos o nodo



La proximidad puede ser por grupo de espacio de archivos o por grupo de nodos. Cuando la proximidad es por grupo de nodos (grupo de asignación de nodos), el servidor intenta asignar datos desde los nodos que pertenecen al mismo grupo de asignación. Un grupo de proximidad de espacio de archivos utiliza los mismos métodos que un grupo de proximidad de nodos, pero puede utilizar más espacio por la granularidad de los tamaños de espacio de archivos. Como se muestra en Figura 2, se han asignado datos para los siguientes grupos de nodos:

- El grupo 1 consta de los nodos A, B y C
- El grupo 2 consta de los nodos D y E
- El grupo 3 consta de los nodos F, G, H e I

Siempre que sea posible, el servidor de IBM Spectrum Protect asigna los datos pertenecientes a un grupo de nodos en una sola cinta, tal como se ve representado en el Grupo 2 de la figura. Los datos de un mismo nodo también se pueden distribuir en varias cintas asociadas a un grupo (Grupo 1 y 2). Si los nodos del grupo de proximidad tienen varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos.

Figura 2. Utilización de todos los volúmenes de almacenamiento de acceso secuencial disponibles con la proximidad habilitada a nivel de grupo



Normalmente, el servidor de IBM Spectrum Protect siempre graba los datos en el volumen de llenado actual para la operación que se está ejecutando. Sin embargo, es posible que en ocasiones detecte más de un volumen de relleno en una agrupación de almacenamiento de proximidad. Puede tener más de un volumen de llenado en una asignación de almacenamiento de proximidad si diferentes procesos de servidor o sesiones de cliente intentan almacenar datos en la agrupación de proximidad al mismo tiempo. En esta situación, IBM Spectrum Protect asigna un volumen para cada proceso o sesión que necesita un volumen, de manera que ambas operaciones se completan lo más rápido posible.

## Selección de volúmenes con proximidad inhabilitada

Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen de almacenamiento antes de acceder a otro volumen.

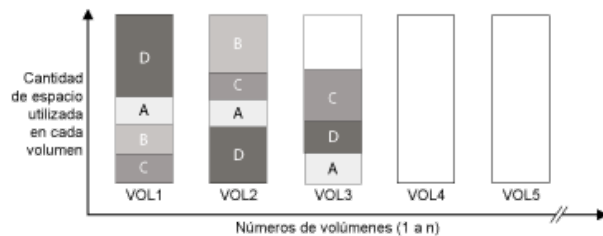
Si almacena archivos de cliente en una agrupación de almacenamiento de acceso secuencial cuando la función de proximidad está inhabilitada, el servidor selecciona un volumen utilizando el siguiente orden de selección:

1. Un volumen secuencial que tenga espacio disponible y que se haya utilizado anteriormente (se selecciona primero el volumen que más datos tiene)
2. Un volumen vacío

Cuando el servidor debe continuar almacenando datos en un segundo volumen, intenta seleccionar un volumen vacío. Si no existe ningún volumen vacío, el servidor intenta seleccionar cualquier volumen disponible que quede en la agrupación de almacenamiento.

Figura 1 muestra que el uso del volumen es vertical cuando la función de proximidad está inhabilitada. En este ejemplo, se utilizan menos volúmenes porque el servidor intenta utilizar todo el espacio disponible mezclando los archivos de clientes en los volúmenes individuales. A, B, C y D representan archivos de cuatro nodos cliente distintos.

Figura 1. Utilización de todo el espacio disponible en volúmenes de acceso secuencial con función de proximidad inhabilitada



## Valores de proximidad

Una vez definida una agrupación de almacenamiento, se puede cambiar el valor de la función de proximidad actualizando la agrupación de almacenamiento. La modificación de la agrupación con respecto a la función de proximidad no afecta a los archivos que ya están almacenados en la agrupación.

Por ejemplo, si la proximidad está desactivada para una agrupación de almacenamiento y la activa, a partir de ese momento se asignan los archivos de cliente que estén almacenados en la agrupación. Los archivos previamente almacenados en la agrupación de almacenamiento no se mueven para asignarse. Cuando se reclamen los volúmenes, los datos de la agrupación tienden a estar más próximos. También puede utilizar los mandatos MOVE DATA o MOVE NODEDATA para mover datos a nuevos volúmenes para incrementar la proximidad. Mover datos a nuevos volúmenes provoca un incremento del tiempo de procesamiento y la actividad de montaje de volúmenes.

Consejo: Se puede producir una espera de montaje o tardar más de lo habitual si la proximidad por espacio de archivo está habilitada y un nodo tiene un volumen que contiene múltiples espacios de archivos. Si un volumen es seleccionable para recibir datos, IBM Spectrum Protect espera a dicho volumen.

## Proximidad de agrupaciones de almacenamiento de copias

En relación con la utilización de la función de proximidad en las agrupaciones de almacenamiento de copia, existen varios aspectos que debe tener en cuenta. La proximidad de agrupaciones de almacenamiento de copia, especialmente por nodo o espacio de archivo, implica más volúmenes parcialmente llenos y actividad de reclamación fuera del local potencialmente innecesaria.

Las agrupaciones de almacenamiento primario tienen un rol de recuperación diferente del de las agrupaciones de almacenamiento de copia. Normalmente, se utilizan las agrupaciones de almacenamiento primario para recuperar datos a los clientes directamente. En caso de desastre, cuando se pierde el servidor y los clientes, puede utilizar volúmenes de agrupación de almacenamiento de copia fuera del sitio para recuperar las agrupaciones de almacenamiento primario. Los tipos de escenarios de recuperación pueden ayudarle a determinar si utilizar la función de proximidad en las agrupaciones de almacenamiento de copia.

La asignación generalmente resulta en el llenado parcial de volúmenes cuando se asigna por nodo o por espacio de archivos. Sin embargo, los volúmenes parcialmente llenos son menos frecuentes cuando aproxima por grupo. Los volúmenes parcialmente llenos se pueden aceptar para agrupaciones de almacenamiento primarias puesto que los volúmenes permanecen disponibles y se pueden llenar durante el siguiente proceso de migración. Sin embargo, los volúmenes parcialmente llenos pueden ser inaceptables para las agrupaciones de almacenamiento de copia cuyos volúmenes de agrupación de almacenamiento se llevan fuera del local de forma inmediata. Si utiliza la función de proximidad para agrupaciones de almacenamiento de copia, debe tomar las siguientes decisiones:

- Mover fuera del sitio más volúmenes parcialmente llenos y aumentar la actividad de reclamación cuando se disminuye o se alcanza el umbral de reclamación.
- Dejar en el local esos volúmenes parcialmente llenos hasta que se llenen y asumir el riesgo de no tener ninguna copia fuera del local de los datos de esos volúmenes.
- Si va a aproximar por grupo para utilizar la máxima capacidad posible de cinta.

Cuando la función de proximidad está inhabilitada para una agrupación de almacenamiento de copia, normalmente solo quedan unos pocos volúmenes parcialmente llenos una vez realizada la copia de seguridad de la agrupación de almacenamiento de copia.

Considere sus opciones detenidamente antes de utilizar la función de proximidad para las agrupaciones de almacenamiento de copia, y si utilizar o no la grabación simultánea. Si no utiliza la grabación simultánea y utiliza la función de proximidad para sus agrupaciones de almacenamiento primario, es posible que desee inhabilitar la función de proximidad para las agrupaciones de almacenamiento de copia. La proximidad de agrupaciones de almacenamiento de copia es recomendable si tiene pocos clientes y cada uno de ellos tiene grandes cantidades de datos de copia de seguridad incremental a diario. Para la proximidad con la grabación simultánea, debe asegurarse de que los parámetros de proximidad sean idénticos para las agrupaciones de almacenamiento primario y las agrupaciones de almacenamiento de copia.

## Planificación y activación de la función de proximidad

Entender los efectos de la función de proximidad puede ayudar a reducir el número de montajes de medios, aprovechar mejor el espacio en volúmenes secuenciales y mejorar la eficacia de las operaciones de servidor.

## Acerca de esta tarea

En la Tabla 1 se enumeran las cuatro opciones de proximidad que puede especificar en los mandatos DEFINE STGPOOL y UPDATE STGPOOL. La tabla muestra los efectos de la proximidad en los datos pertenecientes a los nodos que son miembros de grupos de proximidad y nodos que no son miembros de ningún grupo de proximidad.

Tabla 1. Opciones de proximidad y efectos sobre los datos de los nodos

| Opción de proximidad       | Si un nodo no está definido como miembro de un grupo de proximidad                                                                                                                                                                                                                       | Si un nodo está definido como miembro de un grupo de proximidad                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>No</b>                  | Los datos del nodo no se colocan juntos.                                                                                                                                                                                                                                                 | Los datos del nodo no se colocan juntos.                                                                                                                                                                                                                                                 |
| <b>Grupo</b>               | El servidor almacena los datos del nodo en el menor número posible de volúmenes de la agrupación de almacenamiento.                                                                                                                                                                      | El servidor almacena los datos del nodo y otros nodos que pertenecen al mismo grupo de proximidad en el menor número posible de volúmenes.                                                                                                                                               |
| <b>Nodo</b>                | El servidor almacena los datos del nodo en el menor número posible de volúmenes.                                                                                                                                                                                                         | El servidor almacena los datos del nodo en el menor número posible de volúmenes.                                                                                                                                                                                                         |
| <b>Espacio de archivos</b> | El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento. | El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento. |

Tabla 2. Opciones del grupo de proximidad y efectos sobre los datos de espacio de archivos

| Opción de proximidad       | Si el espacio de archivos no está definido como miembro de un grupo de proximidad                                                                                                                                                                                                        | Si el espacio de archivos está definido como miembro de un grupo de proximidad                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>No</b>                  | Los datos del espacio de archivos no se colocan juntos.                                                                                                                                                                                                                                  | Los datos del espacio de archivos no se colocan juntos.                                                                                                                                                                                                                         |
| <b>Grupo</b>               | El servidor almacena los datos del espacio de archivos en el menor número posible de volúmenes de la agrupación de almacenamiento.                                                                                                                                                       | El servidor almacena los datos del espacio de archivos y otros espacios de archivos que pertenecen al mismo grupo de proximidad en el menor número posible de volúmenes.                                                                                                        |
| <b>Nodo</b>                | El servidor almacena los datos del nodo en el menor número posible de volúmenes.                                                                                                                                                                                                         | El servidor almacena los datos del nodo en el menor número posible de volúmenes.                                                                                                                                                                                                |
| <b>Espacio de archivos</b> | El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento. | El servidor almacena los datos del espacio de archivos en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento. |

## Procedimiento

Para determinar si colocar y cómo los datos, complete los siguientes pasos:

- Determine cómo organizar los datos, si por nodo de cliente, grupo de nodos de cliente o espacio de archivos. Para colocar por grupo, decida cómo agrupar los nodos:
  - Si la finalidad es la de ahorrar espacio, tal vez desee agrupar los nodos pequeños juntos para utilizar mejor las cintas.
  - Si la finalidad es la de agilizar las restauraciones de cliente, agrupe los nodos juntos de forma que completen las menores cintas posible. Al agrupar nodos, los datos de cada nodo se distribuyen en dos o más cintas y así se pueden montar más cintas simultáneamente durante una operación de restauración sin consulta multisesión.
  - Si el objetivo es departamentalizar los datos, puede agrupar los nodos por departamento.
- Para colocar los grupos, complete los siguientes pasos:
  - Defina los grupos de proximidad con el mandato DEFINE COLLOGROUP.
  - Agregar nodos de cliente a los grupos de proximidad con el mandato DEFINE COLLOCMEMBER.

Los mandatos de consulta siguientes están disponibles para ayudarle a aproximar grupos:

QUERY COLLOGROUP

Muestra los grupos de proximidad definidos en el servidor.

#### QUERY NODE

Muestra el grupo de proximidad, si lo hay, al cual pertenece el nodo.

#### QUERY NODEDATA

Muestra información sobre los datos para uno o más nodos en una agrupación de almacenamiento de acceso secuencial.

#### QUERY STGPOOL

Muestra información sobre la ubicación de los datos de cliente en una agrupación de almacenamiento de acceso secuencial, así como de la cantidad de espacio que ocupa un nodo en un volumen.

También puede utilizar los scripts de servidor IBM Spectrum Protect o scripts de Perl para visualizar información que puede ser útil para definir los grupos de proximidad.

3. Especifique cómo colocar los datos en una agrupación de almacenamiento emitiendo el mandato DEFINE STGPOOL o UPDATE STGPOOL y especificando el parámetro COLLOCATE.

## Qué hacer a continuación

---

Recomendación: Para reducir el número de montajes de medios, utilice el espacio en volúmenes secuenciales de forma más eficiente, y habilite la proximidad, complete los pasos siguientes:

- Defina una jerarquía de agrupación de almacenamiento y una política que requiera que los archivos con copia de seguridad, archivados o gestionados por espacio se almacenen inicialmente en agrupaciones de almacenamiento en disco.

Cuando se migran los archivos de una agrupación de almacenamiento de disco, el servidor intenta migrar todos los archivos pertenecientes al nodo de cliente o al grupo de proximidad que utiliza más espacio en disco en la agrupación de almacenamiento. Este proceso funciona bien con la opción de proximidad ya que el servidor intenta colocar todos los archivos de un determinado cliente en el mismo volumen de almacenamiento de acceso secuencial.

- Utilice volúmenes reutilizables para agrupaciones de almacenamiento de acceso secuencial para permitir al servidor seleccionar nuevos volúmenes para la proximidad.
- Especifique la opción de cliente COLLOCATEBYFILESPEC para limitar el número de cintas en las que se deben grabar los objetos asociados con una especificación de archivo. Esta opción de proximidad hace que la función de proximidad del servidor sea más eficaz; no anula la función de proximidad del espacio de archivos ni la del nodo.

## Gestión de dispositivos de cinta

---

Las operaciones rutinarias de cinta incluyen la preparación de volúmenes de cinta para su utilización, controlar cómo y cuándo se reutilizan los volúmenes y asegurarse de que hay suficientes volúmenes disponibles. También debe responder a las solicitudes de operador y gestionar bibliotecas, unidades, discos, vías de acceso y transportadores de datos.

- Preparación de medios extraíbles  
Debe preparar los medios extraíbles antes de utilizarlos para almacenar datos. Las tareas de preparación típicas incluyen el etiquetado y el dar de alta volúmenes.
- Gestión del inventario de volúmenes  
Puede gestionar el inventario de volúmenes controlando el acceso del servidor a los volúmenes, reutilizando las cintas y reutilizando los volúmenes que se utilizan para las operaciones de copia de seguridad de la base de datos y las operaciones de exportación. También puede gestionar el inventario manteniendo un suministro de volúmenes reutilizables.
- Volúmenes grabados parcialmente  
Los volúmenes grabados parcialmente son siempre volúmenes privados, incluso si su estado era reutilizable antes de que el servidor los montara. El servidor realiza el seguimiento del estado original de los volúmenes reutilizables y les devuelve al estado reutilizable cuando están vacíos.
- Operaciones con bibliotecas compartidas  
Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI bibliotecas. La biblioteca física se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas. Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas de IBM Spectrum Protect.
- Gestión de solicitudes del servidor para los volúmenes  
IBM Spectrum Protect muestra solicitudes y mensajes de estado a todos los clientes administrativos de línea de mandato que se han iniciado en modalidad de consola. Estos mensajes de solicitud a menudo tienen un límite de tiempo. Las operaciones satisfactorias de servidor deben completarse dentro del límite de tiempo que se ha especificado; de lo contrario, la operación supera el tiempo de espera

## Preparación de medios extraíbles

---

Debe preparar los medios extraíbles antes de utilizarlos para almacenar datos. Las tareas de preparación típicas incluyen el etiquetado y el dar de alta volúmenes.

## Acerca de esta tarea

---

Cuando IBM Spectrum Protect accede a un volumen de medios extraíbles, verifica el nombre de volumen en la cabecera de la etiqueta para asegurarse de que se ha accedido al volumen correcto.

Los volúmenes de cinta deben estar etiquetados antes de que el servidor pueda utilizarlos.

## Procedimiento

---

Para preparar un volumen para su uso, complete los pasos siguientes:

1. Etiquete el volumen emitiendo el mandato LABEL LIBVOLUME.
2. En el caso de bibliotecas automatizadas, compruebe el volumen de la biblioteca. Para obtener instrucciones, consulte Incorporar volúmenes en una biblioteca automatizada, Recomendación: Si utiliza el mandato LABEL LIBVOLUME con unidades de una biblioteca automatizada, puede etiquetar los volúmenes y darlos de alta en un solo mandato.
3. Si la agrupación de almacenamiento no puede contener los volúmenes reutilizables (MAXSCRATCH=0), identifique el volumen en IBM Spectrum Protect por nombre para que se pueda acceder al volumen más tarde.

Si la agrupación de almacenamiento puede contener volúmenes reutilizables (MAXSCRATCH se establece en un valor distinto de cero), omita este paso.

- Etiquetado de volúmenes de cinta  
Debe etiquetar los volúmenes de cinta antes de que el servidor pueda utilizarlos.
- Incorporar volúmenes en una biblioteca automatizada  
Puede dar de alta un volumen en una biblioteca automatizada utilizando el mandato CHECKIN LIBVOLUME.

## Etiquetado de volúmenes de cinta

---

Debe etiquetar los volúmenes de cinta antes de que el servidor pueda utilizarlos.

## Acerca de esta tarea

---

En el caso de las bibliotecas automatizadas, se le pedirá que inserte el volumen en la ranura de entrada/salida de la biblioteca. Si no hay disponible ninguna estación de entrada/salida (E/S) conveniente, inserte el volumen en una ranura vacía. Puede etiquetar los volúmenes cuando los incorpore o antes de incorporarlos.

## Procedimiento

---

Para etiquetar volúmenes de cinta antes de incorporarlos, lleve a cabo los pasos siguientes:

1. Etiquete los volúmenes de cinta emitiendo el mandato LABEL LIBVOLUME. Por ejemplo, para denominar un volumen de biblioteca VOLUME1 en una biblioteca denominada LIBRARY 1, emita el siguiente mandato:

```
label libvolume library1 volume1
```

Requisito: Debe haber al menos una unidad disponible. La unidad no la puede utilizar otro proceso de IBM Spectrum Protect. Si una unidad está desocupada, se considera que no está disponible.

2. Para sobrescribir una etiqueta existente, especifique el parámetro OVERWRITE=YES. De forma predeterminada, el mandato LABEL LIBVOLUME no graba encima de la etiqueta existente.
- Etiquetado de volúmenes en una SCSI biblioteca  
Puede etiquetar los volúmenes individualmente o bien utilizar IBM Spectrum Protect para buscar volúmenes en la biblioteca y etiquetar los volúmenes encontrados.

### Tareas relacionadas:

Etiquetado de nuevos volúmenes utilizando AUTOLABEL

### Referencia relacionada:

[🔗 LABEL LIBVOLUME \(Etiquetar un volumen de biblioteca\)](#)

## Incorporar volúmenes en una biblioteca automatizada

---



Puede dar de alta un volumen en una biblioteca automatizada utilizando el mandato CHECKIN LIBVOLUME.

## Antes de empezar

---

Para etiquetar automáticamente cintas antes de darlas de alta, emita el mandato DEFINE LIBRARY y especifique el parámetro AUTOLABEL=YES. Utilizando el parámetro AUTOLABEL, se elimina la necesidad de preetiquetar un conjunto de cintas.

## Acerca de esta tarea

---



Los volúmenes que el servidor utiliza para cualquier fin debe tener un nombre exclusivo. Este requisito es válido para todos los volúmenes, tanto si se utilizan para las agrupaciones de almacenamiento como si se emplean para operaciones como una copia de seguridad o exportación de base de datos. El requisito se aplica también a los volúmenes que residen en distintas bibliotecas pero que utiliza el mismo servidor.

Sugerencias:

- No utilice una única biblioteca para los volúmenes que tienen etiquetas de código de barras y volúmenes que no tienen etiquetas de código de barras. La exploración de código de barras puede tardar mucho tiempo para volúmenes no etiquetados.
- El servidor acepta sólo cintas que están etiquetadas con etiquetas estándares IBM®.
- Todos los volúmenes que tienen un código de barras que empieza por CLN se trata como una cinta de limpieza.
- Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

## Procedimiento

---

1. Para dar de alta un volumen de almacenamiento en una biblioteca, emita el mandato CHECKIN LIBVOLUME.  
Consejo: El mandato siempre se ejecuta como un proceso en segundo plano. Espere a que finalice el proceso CHECKIN LIBVOLUME procesando antes de definir volúmenes, o el proceso de definición fallará. Puede ahorrar tiempo si da de alta volúmenes como parte de la operación de etiquetado.
  2. Dé un nombre a la biblioteca y especifique si el volumen es uno privado o reutilizable. En función de si utiliza volúmenes reutilizables o privados, realice uno de los pasos siguientes:
    - Si utiliza únicamente volúmenes reutilizables, compruebe que haya disponibles suficientes volúmenes reutilizables. Por ejemplo, puede necesitar etiquetar más volúmenes. A medida que se utilizan los volúmenes, también puede tener que aumentar el número de volúmenes reutilizables permitidos en la agrupación de almacenamiento definida para esta biblioteca.
    - Si desea utilizar volúmenes privados además o en lugar de volúmenes reutilizables en la biblioteca, defina volúmenes en la agrupación de almacenamiento utilizando el mandato DEFINE VOLUME. Debe etiquetar y dar de alta los volúmenes que defina.
- Incorporar un volumen en una biblioteca SCSI  
Puede dar de alta un volumen emitiendo el mandato CHECKIN LIBVOLUME y especificando el parámetro SEARCH=NO. IBM Spectrum Protect solicita que el operador de montaje cargue el volumen en el puerto de entrada/salida de la biblioteca.
  - Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca  
Cuando tenga muchos volúmenes para dar de alta y desee evitar emitir un mandato CHECKIN LIBVOLUME para cada volumen, puede buscar los nuevos volúmenes en las ranuras de almacenamiento. El servidor ha detectado volúmenes que todavía no se han añadido al inventario de volúmenes.
  - Incorporación de volúmenes desde los puertos de entrada/salida de la biblioteca  
Puede buscar volúmenes etiquetados en todas las ranuras de puertos de entrada/salida en masa y el servidor puede darlos de alta automáticamente.
  - Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas  
Puede ahorrar tiempo al dar de alta volúmenes en las bibliotecas que tengan lectores de códigos de barras utilizando los caracteres de las etiquetas del código de barras como nombres para los volúmenes.
  - Incorporación de volúmenes utilizando un lector de códigos de barras  
Puede ahorrar tiempo al dar de alta volúmenes utilizando un lector de códigos de barras, si la biblioteca tiene uno.
  - Comprobación de volúmenes en una biblioteca completa con intercambio  
Si no hay ranuras vacías disponibles en la biblioteca cuando dé de alta los volúmenes, la operación de registro fallará a menos que se habilite *intercambio*. Si habilita el intercambio y la biblioteca está llena, el servidor seleccionará un volumen para expulsar y, a continuación, da de alta el volumen que ha solicitado.
  -  Sistemas operativos Windows Volúmenes privados y volúmenes reutilizables  
Para optimizar el almacenamiento en cinta, revise la información sobre los volúmenes privados y los volúmenes reutilizables. Utilice los volúmenes privados y los volúmenes reutilizables adecuadamente.
  -  Sistemas operativos Windows Direcciones de elementos para las ranuras de almacenamiento de biblioteca  
Una dirección de elemento es un número que indica la ubicación física de una unidad o ranura de almacenamiento de una biblioteca automatizada.

**Tareas relacionadas:**

## Incorporar un volumen en una biblioteca SCSI

---

Puede dar de alta un volumen emitiendo el mandato CHECKIN LIBVOLUME y especificando el parámetro SEARCH=NO. IBM Spectrum Protect solicita que el operador de montaje cargue el volumen en el puerto de entrada/salida de la biblioteca.

### Procedimiento

---

1. Emita el mandato CHECKIN LIBVOLUME.

Por ejemplo, para dar de alta el volumen VOL001, introduzca el mandato siguiente:

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. Responda a la solicitud del servidor.

- o Si la biblioteca tiene un puerto de entrada/salida, se le solicitará que inserte una cinta en el puerto de entrada/salida.
- o Si la biblioteca no tiene un puerto de entrada/salida, se le solicitará que inserte una cinta en una de las ranuras de la biblioteca. Las direcciones de elementos identifican estas ranuras. Por ejemplo, el servidor detecta que la primera ranura vacía está en la dirección de elemento 5. Se devuelve el siguiente mensaje:

```
ANR8306I 001: Inserte el volumen 8MM VOL001 R/W en la ranura con la dirección de elemento 5 de la biblioteca TAPELIB en no más de 60 minutos; emita 'REPLY' junto con el identificador de solicitud cuando esté preparado.
```

Si no sabe la ubicación de la dirección de elemento 5 en la biblioteca, consulte la hoja de trabajo del dispositivo. Para encontrar la hoja de trabajo, revise la documentación de la biblioteca. Tras insertar el volumen tal como se le ha solicitado, responda al mensaje desde un cliente administrativo de IBM Spectrum Protect. Emita el mandato REPLY, seguido del número de solicitud (el número que aparece el principio de la solicitud de montaje). Por ejemplo:

```
reply 1
```

Consejo: Las direcciones de elementos a veces se numeran empezando por un número distinto de 1. Consulte la hoja de trabajo para estar seguro. Si no se lista ninguna hoja de trabajo para su dispositivo en IBM® Support Portal for IBM Spectrum Protect, consulte la documentación de la biblioteca.

Si especifica un tiempo de espera de 0 utilizando el parámetro opcional WAITTIME en el mandato CHECKIN LIBVOLUME, no es necesario el mandato REPLY. El tiempo de espera predeterminado es de 60 minutos.

## Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca

---

Cuando tenga muchos volúmenes para dar de alta y desee evitar emitir un mandato CHECKIN LIBVOLUME para cada volumen, puede buscar los nuevos volúmenes en las ranuras de almacenamiento. El servidor ha detectado volúmenes que todavía no se han añadido al inventario de volúmenes.

### Procedimiento

---

1. Abra la biblioteca y coloque los nuevos volúmenes en ranuras no utilizadas. Por ejemplo, para un dispositivo SCSI, abra la puerta de acceso de la biblioteca, coloque todos los nuevos volúmenes en ranuras no utilizadas, y cierre la puerta.
2. Si los volúmenes no están etiquetados, utilice el mandato LABEL LIBVOLUME para etiquetar el volumen.
3. Emita el mandato CHECKIN LIBVOLUME con el parámetro SEARCH=YES.

#### Referencia relacionada:

[CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)

## Incorporación de volúmenes desde los puertos de entrada/salida de la biblioteca

---

Puede buscar volúmenes etiquetados en todas las ranuras de puertos de entrada/salida en masa y el servidor puede darlos de alta automáticamente.

### Antes de empezar

---

Emita el mandato LABEL LIBVOLUME para etiquetar volúmenes que no estén etiquetados.

## Acerca de esta tarea

---

Para bibliotecas SCSI, el servidor explora todos los puertos de entrada/salida de la biblioteca buscando volúmenes. Si encuentra un volumen que contiene una etiqueta de volumen válida, se le da de alta automáticamente.

## Procedimiento

---

Emita el mandato CHECKIN LIBVOLUME y especifique el parámetro SEARCH=BULK.

- Para cargar una cinta en una unidad y leer la etiqueta, especifique el parámetro CHECKLABEL=YES. Una vez que el servidor ha leído la etiqueta, desplaza la cinta de la unidad a una ranura de almacenamiento.
- Para que el servidor utilice el lector de códigos de barras para verificar las etiquetas externas de las cintas, especifique el parámetro CHECKLABEL=BARCODE. Cuando está habilitada la lectura de códigos de barras, el servidor lee la etiqueta y desplaza la cinta desde el puerto de entrada/salida a una ranura de almacenamiento.

## Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas

---

Puede ahorrar tiempo al dar de alta volúmenes en las bibliotecas que tengan lectores de códigos de barras utilizando los caracteres de las etiquetas del código de barras como nombres para los volúmenes.

## Acerca de esta tarea

---

El servidor lee las etiquetas de código de barras y utiliza la información para grabar las etiquetas de los medios internos. En el caso de los volúmenes que no tienen etiquetas de código de barras, el servidor monta los volúmenes en una unidad e intenta leer la etiqueta interna grabada.

## Procedimiento

---

Emita el mandato CHECKIN LIBVOLUME con el parámetro CHECKLABEL=BARCODE. Por ejemplo, para utilizar un lector de códigos de barras para buscar en una biblioteca denominada TAPELIB y dar de alta una cinta reutilizable, emita el mandato siguiente:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

## Incorporación de volúmenes utilizando un lector de códigos de barras

---

Puede ahorrar tiempo al dar de alta volúmenes utilizando un lector de códigos de barras, si la biblioteca tiene uno.

## Acerca de esta tarea

---

Cuando dé de alta un volumen, puede especificar si las etiquetas de los medios se leen durante el proceso de incorporación. Si la comprobación de etiquetas está activada, IBM Spectrum Protect monta cada volumen para leer la etiqueta interna y sólo da de alta un volumen si está correctamente etiquetado. La comprobación de etiquetas puede impedir futuros errores cuando se utilizan los volúmenes de las agrupaciones de almacenamiento, pero también aumenta el tiempo de proceso en el registro.

Si un volumen no tiene etiqueta de código de barras, IBM Spectrum Protect monta los volúmenes en una unidad e intenta leer la etiqueta registrada.

## Procedimiento

---

Para dar de volúmenes utilizando un lector de códigos de barras, emita el mandato CHECKIN LIBVOLUME y especifique CHECKLABEL=BARCODE. Por ejemplo, para utilizar el lector de códigos de barras para dar de alta todos los volúmenes como volúmenes reutilizables en una biblioteca denominada TAPELIB, emita el siguiente mandato:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

### Tareas relacionadas:

Preparación de medios extraíbles

### Referencia relacionada:

[CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)

# Comprobación de volúmenes en una biblioteca completa con intercambio

Si no hay ranuras vacías disponibles en la biblioteca cuando dé de alta los volúmenes, la operación de registro fallará a menos que se habilite *intercambio*. Si habilita el intercambio y la biblioteca está llena, el servidor seleccionará un volumen para expulsar y, a continuación, da de alta el volumen que ha solicitado.

## Acerca de esta tarea

El servidor selecciona el volumen de expulsión comprobando primero cualquier volumen reutilizable disponible y, a continuación, para el volumen que está montado con menor frecuencia. El servidor expulsa el volumen que se selecciona para la operación de intercambio de la biblioteca y sustituye el volumen expulsado por el volumen que se está incorporando.

## Procedimiento

Para intercambiar volúmenes si una ranura de biblioteca vacía no está disponible para dar de alta un volumen, emita el mandato CHECKIN LIBVOLUME y especifique el parámetro SWAP=YES. Por ejemplo, al dar de alta un volumen que se denomina VOL1 en una biblioteca que se denomina AUTO y especifica el intercambio, emita el siguiente mandato:

```
checkin libvolume auto voll swap=yes
```

### Tareas relacionadas:

Gestión de una biblioteca completa con una ubicación de desbordamiento

### Referencia relacionada:

 CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

# Volúmenes privados y volúmenes reutilizables

Para optimizar el almacenamiento en cinta, revise la información sobre los volúmenes privados y los volúmenes reutilizables. Utilice los volúmenes privados y los volúmenes reutilizables adecuadamente.

Los volúmenes privados no se pueden sobrescribir cuando se solicita un montaje reutilizable. No se puede dar de alta un volumen con estado reutilizable cuando dicho volumen lo utiliza una agrupación de almacenamiento, para exportar datos, para hacer una copia de seguridad de una base de datos o hacer la copia en un volumen de conjunto de copias de seguridad.

Los volúmenes grabados parcialmente siempre son privados. Los volúmenes tienen un estado de cero o privado, pero cuando IBM Spectrum Protect almacena datos en ellos, su estado pasará a ser privado.

Tabla 1. Usos de los volúmenes privados y los volúmenes reutilizables

| Tipo de volumen         | Cuándo debe utilizarse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volúmenes privados      | Utilice volúmenes privados para regular los volúmenes utilizados por agrupaciones de almacenamiento individuales y para controlar manualmente los volúmenes. Para definir volúmenes privados, emita el mandato DEFINE VOLUME. Para restauraciones de bases de datos, volcados de memoria o cargas, o para las operaciones de importación, debe especificar volúmenes privados.                                                                                                                                                                                                                                                                                                                                |
| Volúmenes reutilizables | En algunos casos, puede simplificar la gestión de volúmenes utilizando volúmenes reutilizables. Puede utilizar volúmenes reutilizables en las siguientes circunstancias: <ul style="list-style-type: none"><li>• Cuando no sea necesario definir cada volumen de agrupación de almacenamiento.</li><li>• Cuando desee aprovechar la automatización de dispositivos robot.</li><li>• Cuando distintas agrupaciones de almacenamiento comparten una biblioteca automatizada y las agrupaciones de almacenamiento pueden adquirir volúmenes de forma dinámica desde los volúmenes reutilizables de la biblioteca. Los volúmenes no tiene que estar preasignados en las agrupaciones de almacenamiento.</li></ul> |

### Tareas relacionadas:

Cambiar el estado de un volumen de una biblioteca automatizada

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

## Direcciones de elementos para las ranuras de almacenamiento de biblioteca

---

Una dirección de elemento es un número que indica la ubicación física de una unidad o ranura de almacenamiento de una biblioteca automatizada.

Si una biblioteca tiene puertos de entrada/salida, puede añadir y eliminar medios utilizando los puertos. Si no existe ningún puerto de entrada/salida, debe cargar cintas en las ranuras de almacenamiento.

Si carga cintas en las ranuras de almacenamiento, debe responder a las solicitudes de montaje que identifican las ranuras de almacenamiento con direcciones de elementos. Si especifica un tiempo de espera de 0 en los mandatos CHECKIN LIBVOLUME o LABEL LIBVOLUME, no es necesario que responda a una solicitud de montaje.

Para direcciones de elemento, consulte la documentación del fabricante del dispositivo o vaya a IBM® Support Portal for IBM Spectrum Protect y busque direcciones de elemento.

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)

## Gestión del inventario de volúmenes



---

Puede gestionar el inventario de volúmenes controlando el acceso del servidor a los volúmenes, reutilizando las cintas y reutilizando los volúmenes que se utilizan para las operaciones de copia de seguridad de la base de datos y las operaciones de exportación. También puede gestionar el inventario manteniendo un suministro de volúmenes reutilizables.

### Acerca de esta tarea

---

Cada volumen que utiliza un servidor debe tener un nombre exclusivo, tanto si los volúmenes se utilizan para las agrupaciones de almacenamiento como si se utilizan para operaciones tales como la copia de seguridad o la exportación de una base de datos. Los volúmenes que residen en distintas bibliotecas pero que utiliza el mismo servidor también tienen que tener un nombre exclusivo.

- Control de acceso a volúmenes  
Puede utilizar distintos métodos para controlar el acceso a los volúmenes.
- Reutilización de cintas  
Para asegurarse un suministro adecuado de cintas, puede caducar archivos antiguos, reclamar volúmenes y suprimir volúmenes que alcanzan el final de su vida. También puede mantener un suministro de volúmenes reutilizables.
- Mantenimiento de un suministro de volúmenes reutilizables  
Debe establecer el número máximo de volúmenes reutilizables para una agrupación de almacenamiento lo suficientemente grande para el uso estimado.
-  Sistemas operativos AIX  Sistemas operativos Linux Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM  
En el caso de las bibliotecas que contienen medios WORM (Write Once Read Many), puede impedir que se cancelen transacciones de almacenamiento de datos manteniendo un suministro de volúmenes privados nuevos o reutilizables en la biblioteca. La cancelación de transacciones puede hacer que se pierdan medios WORM.
- Gestión del inventario de volumen en bibliotecas automatizadas  
El servidor de IBM Spectrum Protect utiliza un inventario de volúmenes de biblioteca para realizar el seguimiento de los volúmenes reutilizables y privados disponibles en una biblioteca automatizada. Debe asegurarse de que el inventario es coherente con los volúmenes que están físicamente en la biblioteca.

## Control de acceso a volúmenes

---

Puede utilizar distintos métodos para controlar el acceso a los volúmenes.

### Procedimiento

---

Para controlar el acceso a los volúmenes, realice cualquiera de las siguientes acciones:

- Para impedir que el servidor monte un volumen, emita el mandato UPDATE VOLUME y especifique el parámetro ACCESS=UNAVAILABLE.
- Para convertir a los volúmenes en no disponibles y enviarlos a otro lugar para su protección, utilice una agrupación de almacenamiento de copias o una agrupación de almacenamiento de datos activos.
- Puede hacer copia de seguridad de las agrupaciones de almacenamiento primarias en una agrupación de almacenamiento de copias y después enviar los volúmenes de la agrupación de almacenamiento de copias fuera del local.
- Puede copiar versiones activas de los datos de copia de seguridad de cliente en agrupaciones de almacenamiento de datos activos y, a continuación, enviar los volúmenes a otro lugar.
- Puede hacer el seguimiento de los volúmenes de agrupación de almacenamiento de copias y los volúmenes de agrupación de datos activos cambiando la modalidad de acceso a fuera del local y actualizando el histórico de volúmenes para identificar su ubicación.

**Referencia relacionada:**

➔ UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

## Reutilización de cintas

---

Para asegurarse un suministro adecuado de cintas, puede caducar archivos antiguos, reclamar volúmenes y suprimir volúmenes que alcanzan el final de su vida. También puede mantener un suministro de volúmenes reutilizables.

### Acerca de esta tarea

---

A lo largo del tiempo, los medios envejecen, y es posible que no necesite algunos de los datos de copia de seguridad almacenados en ellos. Puede definir políticas de servidor para determinar cuántas versiones de copia de seguridad se retienen y cuánto tiempo se retienen. Puede utilizar el proceso de caducidad para suprimir archivos que ya no necesite. Puede guardar los datos que necesite en los medios. Cuando ya no los necesite, puede reclamar y reutilizar los medios.

### Procedimiento

---

1. Suprima los datos de clientes no necesarios ejecutando regularmente el proceso de caducidad. El proceso de caducidad suprime los datos que ya no son válidos porque superan las especificaciones de retención de la política o porque los usuarios o los administradores han suprimido las versiones activas de los datos.
2. Reutilice los volúmenes de las agrupaciones de almacenamiento ejecutando el proceso de reclamación.

El proceso de reclamación consolida todos los datos sin caducar traspasándolos de un gran número de volúmenes a un número menor de volúmenes. A continuación, es posible devolver los medios a la agrupación de almacenamiento y reutilizarlos.

3. Puede reutilizar volúmenes que contengan copias de seguridad de bases de datos obsoletas o datos exportados que ya no sean necesarios suprimiendo el historial de volumen.

Para que el servidor pueda reutilizar volúmenes de los que se realiza un seguimiento en el historial de volumen, debe suprimir la información de volúmenes del archivo de historial de volumen emitiendo el mandato DELETE VOLHISTORY.

Consejo: Si el servidor utiliza la función gestor recuperación tras desastre (DRM), la información del volumen se suprime automáticamente durante el proceso del mandato MOVE DRMEDIA.

4. Determine cuándo alcanzan los volúmenes de cinta el final de su vida. Puede utilizar el servidor para visualizar las estadísticas acerca de los volúmenes, incluidos el número de operaciones de grabación completadas en el medio y el número de errores de grabación. Los volúmenes privados y los volúmenes reutilizables muestran los siguientes datos estadísticos:

**Volúmenes privados**

Para los medios inicialmente definidos como volúmenes privados, el servidor mantiene estos datos estadísticos, incluso aunque se reclame el volumen. Puede comparar la información con el número de operaciones y errores de grabación recomendado por el fabricante.

**Volúmenes reutilizables**

Para los medios inicialmente definidos como volúmenes reutilizables, el servidor sobrescribe estos datos estadísticos cada vez que se reclamen los volúmenes.

5. Reclame cualquier dato válido de los volúmenes que alcanzan el final de su vida. Si los volúmenes están en bibliotecas automatizadas, delos de baja del inventario de volúmenes. Suprima los volúmenes privados de la base de datos con el mandato DELETE VOLUME.
6. Asegúrese de que los volúmenes estén disponibles para la rotación de cintas de modo que la agrupación de almacenamiento no se quede sin espacio. Puede utilizar el Centro de operaciones para supervisar la disponibilidad de los volúmenes reutilizables. Asegúrese de que el número de volúmenes reutilizables sea lo suficientemente grande como para satisfacer la demanda. Para

obtener más información, consulte Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM.

medios WORM: Las unidades WORM (una sola grabación, varias lecturas) pueden desperdiciar medios si el servidor cancela transacciones por no encontrarse los volúmenes disponibles para completar la operación de copia seguridad. Una vez que el servidor grabe en los volúmenes WORM, el estado de los volúmenes no se puede reutilizar, incluso aunque se hayan cancelado las transacciones (por ejemplo, si se cancela una copia de seguridad debido a la falta de medios en el dispositivo). Para minimizar los medios WORM desperdiciados, realice las acciones siguientes:

- a. Asegúrese de que el número máximo de volúmenes reutilizables para la agrupación de almacenamiento es, como mínimo, equivalente al número de ranuras de almacenamiento de la biblioteca.
- b. Dé de alta suficientes volúmenes en el inventario de volúmenes del dispositivo para la carga prevista.

Si la mayoría de operaciones de copia de seguridad son para archivos pequeños, el control del tamaño de las transacciones puede afectar a la forma como se utilizan los discos WORM. Las transacciones más pequeñas significa que se desperdicia menos espacio cuando una transacción como una operación de copia de seguridad debe ser cancelada. El tamaño de transacción lo controlan una opción de servidor, TXNGROUPMAX, y una opción de cliente, TXNBYTELIMIT.

**Tareas relacionadas:**

Migración de datos a unidades actualizadas  
Gestión de solicitudes del servidor para los volúmenes

**Referencia relacionada:**

- ➔ DELETE VOLHISTORY (Suprimir información histórica de volúmenes secuencial)
- ➔ DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)
- ➔ Opción Txnbytelimit
- ➔ TXNGROUPMAX, opción de servidor

**Información relacionada:**

- ➔ EXPIRE INVENTORY (Iniciar manualmente el proceso de caducidad de inventario)

## Mantenimiento de un suministro de volúmenes reutilizables

---

Debe establecer el número máximo de volúmenes reutilizables para una agrupación de almacenamiento lo suficientemente grande para el uso estimado.

### Acerca de esta tarea

---

En el momento de definir una agrupación de almacenamiento, debe especificarse el número máximo de volúmenes reutilizables que puede utilizar la misma. El servidor solicita automáticamente un volumen reutilizable cuando es necesario. Si el número de volúmenes reutilizables que el servidor está utilizando para la agrupación de almacenamiento sobrepasa el máximo especificado, es posible que la agrupación de almacenamiento se quede sin espacio.

### Procedimiento

---

Cuando una agrupación de almacenamiento necesita más que el número máximo de volúmenes reutilizables, puede seguir una o ambas de las acciones siguientes:

1. Aumentar el número máximo de volúmenes reutilizables emitiendo el mandato UPDATE STGPOOL y especificando el parámetro MAXSCRATCH.
2. Consiga volúmenes disponibles para su reutilización ejecutando el proceso de caducidad y el de reclamación a fin de consolidar los datos en menos volúmenes.
  - a. Emita el mandato EXPIRE INVENTORY para ejecutar el proceso de caducidad.  
Consejo: De forma predeterminada este proceso se ejecuta cada día automáticamente. También puede especificar la opción de servidor EXPINTERVAL en el archivo de opciones del servidor, dsmserv.opt, para ejecutar el proceso de caducidad automáticamente. Si el valor es 0 significa que debe utilizar el mandato EXPIRE INVENTORY para ejecutar el proceso de caducidad.
  - b. Emita el mandato RECLAIM STGPOOL para ejecutar el proceso de reclamación.  
Consejo: También puede especificar umbrales de reclamación cuando defina la agrupación de almacenamiento utilizando el mandato DEFINE STGPOOL y especificando el parámetro RECLAIMPROCESS.

### Qué hacer a continuación

---

Si necesita más volúmenes para futuras operaciones de copia de seguridad, etiquete más volúmenes reutilizables utilizando el mandato LABEL LIBVOLUME.

**Tareas relacionadas:**

Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada

**Referencia relacionada:**



- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

**Información relacionada:**

- ➔ EXPIRE INVENTORY (Iniciar manualmente el proceso de caducidad de inventario)
- ➔ RECLAIM STGPOOL (Reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial)

## Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM

---

En el caso de las bibliotecas que contienen medios WORM (Write Once Read Many), puede impedir que se cancelen transacciones de almacenamiento de datos manteniendo un suministro de volúmenes privados nuevos o reutilizables en la biblioteca. La cancelación de transacciones puede hacer que se pierdan medios WORM.

### Acerca de esta tarea

---

IBM Spectrum Protect cancela una transacción si los volúmenes, ya sean privados o reutilizables, no están disponibles para completar la operación de almacenamiento de datos. Una vez que IBM Spectrum Protect empieza una transacción y graba en un volumen WORM, el espacio grabado del volumen no puede volverse a utilizar aunque se cancele la transacción.

Por ejemplo, si tiene volúmenes WORM que tienen 2,6 GB cada uno de ellos y un cliente empieza a hacer copia de seguridad de un archivo de 12 GB. Si IBM Spectrum Protect no puede adquirir un quinto volumen reutilizable después de que cuatro volúmenes estén llenos, IBM Spectrum Protect cancela la operación de copia de seguridad. Los cuatro volúmenes que IBM Spectrum Protect ya ha llenado no se pueden volver a utilizar.

Para minimizar la cancelación de transacciones, debe disponer de suficientes volúmenes disponibles en la biblioteca para gestionar operaciones de cliente esperadas como, por ejemplo, copias de seguridad.

### Procedimiento

---

1. Asegúrese de que la agrupación de almacenamiento asociada con la biblioteca tenga suficientes volúmenes reutilizables. Emita el mandato UPDATE STGPOOL y especifique el parámetro MAXSCRATCH.
2. Para gestionar la carga esperada, dé de alta un número suficiente de volúmenes privados o reutilizables en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME.
3. Para controlar el tamaño de la transacción, especifique la opción de servidor TXNGROUPMAX y la opción de cliente TXNBYTELIMIT. Si los clientes tienden a almacenar archivos pequeños, el control del tamaño de las transacciones puede afectar al uso de los volúmenes WORM. Las transacciones más pequeñas desperdician menos espacio cuando se debe cancelar una transacción como una copia de seguridad.

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)
- ➔ Opción Txnbytelimit
- ➔ TXNGROUPMAX, opción de servidor

## Gestión del inventario de volumen en bibliotecas automatizadas

---

El servidor de IBM Spectrum Protect utiliza un inventario de volúmenes de biblioteca para realizar el seguimiento de los volúmenes reutilizables y privados disponibles en una biblioteca automatizada. Debe asegurarse de que el inventario es coherente con los volúmenes que están físicamente en la biblioteca.

El inventario de volúmenes de biblioteca es independiente del inventario de volúmenes de cada agrupación de almacenamiento. Para añadir un volumen a un inventario de volúmenes de biblioteca, incorpore un volumen a dicha biblioteca de IBM Spectrum Protect.

Una lista de los volúmenes en el inventario de volúmenes de la biblioteca puede no ser idéntica a una lista de volúmenes en el inventario de agrupación de almacenamiento del dispositivo. Por ejemplo, puede dar de alta volúmenes reutilizables a la biblioteca pero no puede definirlos en una agrupación de almacenamiento. Si no se seleccionan volúmenes reutilizables para las operaciones de copia de seguridad, puede definir los volúmenes privados en una agrupación de almacenamiento pero no puede darlos de alta en el inventario de volúmenes para el dispositivo.

Para garantizar que el inventario de volúmenes de la biblioteca del servidor sea exacto, debe dar de baja los volúmenes para eliminarlos físicamente de una biblioteca SCSI. Cuando se da de baja un volumen que utiliza una agrupación de almacenamiento, el volumen permanece en la agrupación de almacenamiento. Si debe montar el volumen cuando se ha extraído, se mostrará un mensaje



en la consola del operador de montaje con una solicitud para dar de alta el volumen. Si la operación de dar de alta no es correcta, el servidor marcará el volumen como no disponible.

Cuando un volumen está en el inventario de volúmenes de biblioteca, puede cambiar su estado de reutilizable a privado.

Para comprobar si el inventario de volumen para la biblioteca del servidor es coherente con los volúmenes que se encuentran físicamente en la biblioteca, puede auditar la biblioteca. El inventario puede volverse inexacto si los volúmenes se mueven dentro y fuera de la biblioteca sin informar al servidor utilizando las operaciones de dar de alta o de dar de baja volúmenes.

- Cambiar el estado de un volumen de una biblioteca automatizada  
Puede cambiar el estado de un volumen de privado a reutilizable o de reutilizable a privado.
- Eliminación de volúmenes de una biblioteca automatizada  
Puede eliminar volúmenes de una biblioteca automatizada si ha exportado los datos a un volumen y desea importar los datos a otro sistema. También es posible que desee eliminar volúmenes para crear espacio para nuevos volúmenes.
- Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada  
Al definir una agrupación de almacenamiento asociada con una biblioteca automatizada, puede especificarse un número máximo de volúmenes reutilizables que sea igual a la capacidad física de la biblioteca. Si el servidor utiliza un número mayor de volúmenes reutilizables para la agrupación de almacenamiento, debe asegurarse de que hay suficientes volúmenes disponibles.
- Gestión de una biblioteca completa con una ubicación de desbordamiento  
Como aumenta la demanda de almacenamiento, el número de volúmenes que necesita para una agrupación de almacenamiento puede superar la capacidad física de una biblioteca automatizada. Para crear espacio disponible para nuevos volúmenes y para supervisar los volúmenes existentes, puede definir una ubicación de desbordamiento para una agrupación de almacenamiento.
- Auditoría de inventarios de volúmenes en una biblioteca  
Puede auditar una biblioteca automatizada para asegurarse de que el inventario de volúmenes de biblioteca es coherente con los volúmenes que están físicamente en la biblioteca. Es posible que desee auditar una biblioteca si el inventario de volúmenes de biblioteca se ha distorsionado debido al traspaso manual de volúmenes en la biblioteca o a problemas con la base de datos.

**Tareas relacionadas:**

Incorporar volúmenes en una biblioteca automatizada

**Referencia relacionada:**

[AUDIT LIBRARY](#) (Inventarios de volúmenes de auditoría en una biblioteca automatizada)

## Cambiar el estado de un volumen de una biblioteca automatizada

---

Puede cambiar el estado de un volumen de privado a reutilizable o de reutilizable a privado.

### Procedimiento

---

Para cambiar el estado de un volumen, emita el mandato UPDATE LIBVOLUME. Por ejemplo, para cambiar el estado de un volumen que se denomina VOL1 a un volumen privado, emita el siguiente mandato:

```
update libvolume lib1 voll status=private
```

Restricciones:

- No puede cambiar el estado de un volumen de privado a reutilizable si el volumen pertenece a una agrupación de almacenamiento o se define en el archivo histórico de volúmenes.
- Los volúmenes privados deben ser volúmenes definidos por el administrador, ya sea sin datos o con datos no válidos. No pueden ser volúmenes grabados parcialmente que contienen datos activos. Las estadísticas de los volúmenes se pierden cuando se modifican los estados de los volúmenes.

## Eliminación de volúmenes de una biblioteca automatizada

---

Puede eliminar volúmenes de una biblioteca automatizada si ha exportado los datos a un volumen y desea importar los datos a otro sistema. También es posible que desee eliminar volúmenes para crear espacio para nuevos volúmenes.

### Acerca de esta tarea

---

De forma predeterminada, el servidor monta el volumen que se extrae y verifica la etiqueta interna. Una vez comprobada la etiqueta, el servidor elimina el volumen del inventario de volúmenes de la biblioteca y, seguidamente, lo traslada al puerto de entrada/salida o a la estación de E/S de la biblioteca que convenga. Si la biblioteca no tiene un puerto de entrada/salida, el servidor solicita que el operador de montaje elimine el volumen de una ranura o dispositivo dentro de la biblioteca.

### Procedimiento

---

- Para eliminar un volumen de una biblioteca automatizada, emita el mandato CHECKOUT LIBVOLUME.
- Para las bibliotecas automatizadas con varios puertos de entrada/salida, emita el mandato CHECKOUT LIBVOLUME y especifique el parámetro REMOVE=BULK. El servidor expulsa el volumen al siguiente puerto de entrada/salida disponible.

## Qué hacer a continuación

---

Si da de baja un volumen definido en una agrupación de almacenamiento y el servidor debe acceder más tarde al volumen, el servidor requiere que se dé de alta el volumen. Para devolver volúmenes a una biblioteca, emita el mandato CHECKIN LIBVOLUME.

### Referencia relacionada:

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

## Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada

---

Al definir una agrupación de almacenamiento asociada con una biblioteca automatizada, puede especificarse un número máximo de volúmenes reutilizables que sea igual a la capacidad física de la biblioteca. Si el servidor utiliza un número mayor de volúmenes reutilizables para la agrupación de almacenamiento, debe asegurarse de que hay suficientes volúmenes disponibles.

## Procedimiento

---

Si el número de volúmenes reutilizables que el servidor está utilizando para la agrupación de almacenamiento sobrepasa el número que se especifica en la definición de la agrupación de almacenamiento, lleve a cabo los pasos siguientes:

1. Puede añadir volúmenes reutilizables a la biblioteca emitiendo el mandato CHECKIN LIBVOLUME.  
Consejo: Puede que tenga que utilizar una ubicación suplementaria para sacar volúmenes de la biblioteca y dejar sitio para los volúmenes reutilizables. Para obtener más información, consulte Gestión de una biblioteca completa con una ubicación de desbordamiento.
2. Aumentar el número máximo de volúmenes reutilizables que se pueden añadir a una agrupación de almacenamiento emitiendo el mandato UPDATE STGPOOL y especificando el parámetro MAXSCRATCH.

## Qué hacer a continuación

---

Es posible que necesite más volúmenes para futuras operaciones de recuperación, de modo que tenga en cuenta etiquetar y apartar volúmenes reutilizables adicionales.

### Tareas relacionadas:

Mantenimiento de un suministro de volúmenes reutilizables

## Gestión de una biblioteca completa con una ubicación de desbordamiento

---

Como aumenta la demanda de almacenamiento, el número de volúmenes que necesita para una agrupación de almacenamiento puede superar la capacidad física de una biblioteca automatizada. Para crear espacio disponible para nuevos volúmenes y para supervisar los volúmenes existentes, puede definir una ubicación de desbordamiento para una agrupación de almacenamiento.

## Acerca de esta tarea

---

El servidor realiza un seguimiento de los volúmenes que se mueven al área de desbordamiento y hace que las ranuras de almacenamiento estén disponibles para nuevos volúmenes.

## Procedimiento

---

1. Cree una ubicación de desbordamiento de un volumen. Defina o actualice la agrupación de almacenamiento asociada con la biblioteca automatizada emitiendo el mandato DEFINE STGPOOL o UPDATE STGPOOL y especificando el parámetro OVFLLOCATION. Por ejemplo, para crear una ubicación de desbordamiento denominada ROOM2948 para una agrupación de almacenamiento denominada ARCHIVEPOOL, emita el siguiente mandato:  

```
update stgpool archivepool ovflocation=Room2948
```
2. Cuando necesite crear espacio en la biblioteca para los volúmenes reutilizables, mueva volúmenes completos a la ubicación de desbordamiento emitiendo el mandato MOVE MEDIA. Por ejemplo, para mover todos los volúmenes completos de la agrupación de almacenamiento especificada fuera de la biblioteca, emita el siguiente mandato:

```
move media * stgpool=archivepool
```

3. Dé de alta los volúmenes reutilizables según sea necesario.

Restricción: Si un volumen tiene una entrada en el archivo histórico de volúmenes, no puede darlo de alta como volumen reutilizable. Para obtener más información, consulte Incorporar volúmenes en una biblioteca automatizada.

4. Identifique las cintas reutilizables vacías de la ubicación de desbordamiento emitiendo el mandato QUERY MEDIA. Por ejemplo, emita el siguiente mandato:

```
query media * stg=* whereovflocation=Room2948 wherestatus=empty
```

5. Si el servidor solicita volúmenes adicionales, localice y dé de alta los volúmenes desde la ubicación de desbordamiento.

Para buscar volúmenes en una ubicación de desbordamiento, emita el mandato QUERY MEDIA. También puede utilizar el mandato QUERY MEDIA para generar mandatos para dar de alta volúmenes.

Por ejemplo, para listar los volúmenes de la ubicación de desbordamiento y a la vez generar los mandatos para dar de alta esos volúmenes en la biblioteca, emita un mandato parecido al del siguiente ejemplo:

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948
cmd="checkin libvol autolib &vol status=private"
cmdfilename="\storage\move\media\checkin.vols"
```

Sugerencias:

- o Las solicitudes de montaje del servidor incluyen la ubicación de los volúmenes.
- o Para especificar el número de días que deben transcurrir hasta que los volúmenes sean elegibles para su procesamiento, emita el mandato UPDATE STGPOOL y especifique el parámetro REUSEDELAY.
- o El archivo que contiene los mandatos generados se puede ejecutar utilizando el mandato MACRO de IBM Spectrum Protect.

#### Referencia relacionada:

- [MOVE MEDIA](#) (Trasladar medios de agrupación de almacenamiento de acceso secuencial)
- [QUERY MEDIA](#) (Consultar un medio de agrupación de almacenamiento de acceso secuencial)
- [UPDATE STGPOOL](#) (Actualizar una agrupación de almacenamiento)

## Auditoría de inventarios de volúmenes en una biblioteca

---

Puede auditar una biblioteca automatizada para asegurarse de que el inventario de volúmenes de biblioteca es coherente con los volúmenes que están físicamente en la biblioteca. Es posible que desee auditar una biblioteca si el inventario de volúmenes de biblioteca se ha distorsionado debido al traspaso manual de volúmenes en la biblioteca o a problemas con la base de datos.

### Procedimiento

---

1. Asegúrese de que no haya volúmenes montados en las unidades de biblioteca. Si hay algún volumen montado en estado IDLE, emita el mandato DISMOUNT VOLUME para desmontarlo.
2. Audite el inventario de volumen emitiendo el mandato AUDIT LIBRARY. Realice una de las siguientes acciones:
  - o Si la biblioteca tiene un lector de códigos de barras, puede ahorrar tiempo utilizando el lector de códigos de barras para identificar volúmenes. Por ejemplo, para auditar la biblioteca TAPELIB mediante su lector de códigos de barras, emita el siguiente mandato:

```
audit library tapelib checklabel=barcode
```

- o Si la biblioteca no tiene un lector de códigos de barras, emita el mandato AUDIT LIBRARY sin especificar CHECKLABEL=BARCODE. El servidor monta cada volumen para verificar la etiqueta. Una vez verificada la etiqueta, el servidor finaliza la auditoría de los volúmenes restantes.

### Resultados

---

El servidor suprime los volúmenes ausentes del inventario y actualiza las ubicaciones de los volúmenes que se han movido desde la última auditoría.

Restricción: El servidor no puede agregar volúmenes nuevos al inventario durante una operación de auditoría.

#### Tareas relacionadas:

Etiquetado de volúmenes de cinta

#### Referencia relacionada:

- [AUDIT LIBRARY](#) (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- [DISMOUNT VOLUME](#) (Desmontar un volumen por nombre de volumen)

## Volúmenes grabados parcialmente

Los volúmenes grabados parcialmente son siempre volúmenes privados, incluso si su estado era reutilizable antes de que el servidor los montara. El servidor realiza el seguimiento del estado original de los volúmenes reutilizables y les devuelve al estado reutilizable cuando están vacíos.

Excepto los volúmenes en las bibliotecas automatizadas, el servidor no reconoce un volumen reutilizable hasta que el volumen no está montado. A continuación, el estado del volumen cambia a privado y el volumen se define automáticamente como componente de la agrupación de almacenamiento para la que se ha efectuado la solicitud de montaje.

### Tareas relacionadas:

Cambiar el estado de un volumen de una biblioteca automatizada

## Operaciones con bibliotecas compartidas

Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI bibliotecas. La biblioteca física se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas. Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas de IBM Spectrum Protect.

El cliente de biblioteca se pone en contacto con el gestor de bibliotecas cuando este se inicia y el dispositivo de almacenamiento se inicializa, o después de definir un gestor de bibliotecas para un cliente de biblioteca. El cliente de biblioteca confirma que el servidor contactado es el gestor de bibliotecas para el dispositivo de biblioteca especificado. El cliente de biblioteca también compara con el gestor de bibliotecas las definiciones de unidades para comprobar que son coherentes. El cliente de biblioteca se pone en contacto con el gestor de biblioteca para cada una de las operaciones siguientes:

### Montaje de un volumen

Un cliente de biblioteca envía una solicitud al gestor de biblioteca para acceder a un volumen en el dispositivo de biblioteca compartida. Para un volumen reutilizable, el cliente de biblioteca no especifica un nombre de volumen. Si el gestor de bibliotecas no puede acceder al volumen solicitado, o si los volúmenes reutilizables no están disponibles, el gestor de bibliotecas deniega la solicitud de montaje. Si la operación de montaje es correcta, el gestor de bibliotecas devuelve el nombre de la unidad en el que está montado el volumen.

### Liberación de un volumen

Cuando un cliente de biblioteca ya no necesita acceder a un volumen, notifica al gestor de bibliotecas que el volumen se puede retornar a volumen reutilizable. La base de datos del gestor de bibliotecas se actualiza con la nueva ubicación del volumen, que es ahora el inventario del servidor de biblioteca. El volumen se suprime del inventario de volumen del cliente de biblioteca.

En la Tabla 1 se muestra la interacción entre los clientes de biblioteca y el gestor de bibliotecas al procesar las operaciones de IBM Spectrum Protect.

Tabla 1. Cómo procesan los servidores habilitados para SAN las operaciones de IBM Spectrum Protect

| Operación<br>(mandato)                                                                       | Gestor de bibliotecas                                                                                                               | Cliente de biblioteca                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Consultar volúmenes de biblioteca<br><br>(QUERY LIBVOLUME)                                   | Muestra los volúmenes dados de alta en la biblioteca. En el caso de volúmenes privados, también se muestra el servidor propietario. | No aplicable.                                                                                                                                                                              |
| Dar de alta y de baja volúmenes de biblioteca<br><br>(CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME) | Envía los mandatos al dispositivo de biblioteca.                                                                                    | No aplicable.<br><br>Cuando se requiere una operación de dar de alta a causa de una operación de restauración de un cliente, se envía una solicitud al servidor del gestor de bibliotecas. |

| <b>Operación (mandato)</b>                                                   | <b>Gestor de bibliotecas</b>                                                                                                               | <b>Cliente de biblioteca</b>                                                                                                              |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Trasladar medios y trasladar medios de DRM<br><br>(MOVE MEDIA, MOVE DRMEDIA) | Válido sólo para los volúmenes que utiliza el servidor del gestor de bibliotecas.                                                          | Solicita que el servidor del gestor de bibliotecas complete la operación. Genera un proceso de baja en el servidor gestor de bibliotecas. |
| Auditar inventario de biblioteca<br><br>(AUDIT LIBRARY)                      | Sincroniza el inventario con el dispositivo de biblioteca.                                                                                 | Sincroniza el inventario con el servidor del gestor de bibliotecas.                                                                       |
| Etiquetar un volumen de biblioteca<br><br>(LABEL LIBVOLUME)                  | Etiqueta y da de alta los volúmenes.                                                                                                       | No aplicable.                                                                                                                             |
| Desmontar un volumen<br><br>(DISMOUNT VOLUME)                                | Envía la solicitud al dispositivo de biblioteca.                                                                                           | Solicita que el servidor del gestor de bibliotecas complete la operación.                                                                 |
| Consultar un volumen<br><br>(QUERY VOLUME)                                   | Comprueba si el volumen es propiedad del cliente de biblioteca solicitante y comprueba si el volumen está en el dispositivo de biblioteca. | Solicita que el servidor del gestor de bibliotecas complete la operación.                                                                 |

## Gestión de solicitudes del servidor para los volúmenes

IBM Spectrum Protect muestra solicitudes y mensajes de estado a todos los clientes administrativos de línea de mandato que se han iniciado en modalidad de consola. Estos mensajes de solicitud a menudo tienen un límite de tiempo. Las operaciones satisfactorias de servidor deben completarse dentro del límite de tiempo que se ha especificado; de lo contrario, la operación supera el tiempo de espera.

### Acerca de esta tarea

En las bibliotecas automatizadas, utilice los mandatos CHECKIN LIBVOLUME y LABEL LIBVOLUME para insertar cartuchos en ranuras. Si se especifica un valor para el parámetro WAITTIME, se muestra un mensaje de respuesta. Si el valor del parámetro es 0, no hace falta respuesta alguna. Cuando emite el mandato CHECKOUT LIBVOLUME, debe insertar cartuchos en las ranuras y, en todos los casos, se muestra un mensaje de respuesta.

### Procedimiento


La tabla siguiente proporciona información acerca de cómo manejar diferentes tareas de soportes del servidor.

| <b>Tarea</b>                                                | <b>Detalles</b>                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Utilizar el cliente administrativo para mensajes de montaje | <p>El servidor envía mensajes de estado de la solicitud de montaje a la consola del servidor y a todos los clientes administrativos de línea de mandatos en modalidad de montaje o de consola.</p> <p>Para iniciar un cliente administrativo de línea de mandatos en modalidad de montaje, emita el mandato dsmadmc -mountmode en el cliente administrativo de línea de mandatos.</p> |

| Tarea                                                                | Detalles                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recibir mensajes sobre las bibliotecas automatizadas                 | Puede ver mensajes de montaje y mensajes de error sobre las bibliotecas automatizadas en los clientes administrativos de línea de mandatos en modalidad de montaje o de consola. Los mensajes de montaje se envían a la biblioteca y no a un operador. La información relativa a problemas con la biblioteca se envían a la cola de mensajes de montaje.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Obtenga información acerca de las solicitudes de operador pendientes | Para obtener información acerca de las solicitudes de operador pendientes, utilice el mandato QUERY REQUEST o consulte la cola de mensajes de montaje de un cliente administrativo de línea de mandatos iniciado en modalidad de montaje. Cuando emita el mandato QUERY REQUEST, el servidor muestra las acciones solicitadas y la cantidad de tiempo que queda antes de que las solicitudes superen el tiempo de espera.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Responder a las solicitudes de operador                              | <p>Si el servidor requiere una respuesta explícita al completarse una solicitud de montaje, utilice el mandato REPLY.</p> <p>El parámetro <i>número_solicitud</i> especifica el número de identificación de solicitud que indica al servidor cuál de las operaciones de operador pendientes se ha completado. Este número de tres dígitos se visualiza siempre como parte del mensaje de solicitud.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cancelar una solicitud de operador                                   | <p>Para cancelar una solicitud de montaje para una biblioteca, emita el mandato CANCEL REQUEST. Para la mayoría de las solicitudes asociadas con las bibliotecas SCSI automatizadas, un operador debe completar una acción de hardware o del sistema para cancelar el montaje solicitado. En este tipo de solicitudes, el servidor no acepta el mandato CANCEL REQUEST.</p> <p>El mandato CANCEL REQUEST debe incluir el número de identificación de la solicitud. Este número está incluido en el mensaje de solicitud.</p> <p>Si desea marcar el volumen solicitado como UNAVAILABLE, emita el mandato CANCEL REQUEST y especifique el parámetro PERMANENT. Si especifica el parámetro PERMANENT, el servidor no intentará montar el volumen solicitado de nuevo. Esto es útil si, por ejemplo, el volumen está en un sitio remoto o si no está disponible.</p>                                                                                                                                                                               |
| Responder a una solicitud para dar de alta el volumen                | <p>Si el servidor no encuentra un volumen determinado que debe montarse en una biblioteca automatizada, el servidor pide que el operador dé de alta el volumen.</p> <p>Si el volumen solicitado está disponible, colóquelo en la biblioteca y efectúe el alta. Para obtener más información, consulte Incorporar volúmenes en una biblioteca automatizada.</p> <p>Si el volumen solicitado no está disponible, actualice la modalidad de acceso del volumen emitiendo el mandato UPDATE VOLUME y especificando el parámetro ACCESS=UNAVAILABLE. A continuación, cancele la solicitud de alta utilizando el mandato CANCEL REQUEST. No cancele el proceso de cliente que ha originado la solicitud. Utilice el mandato QUERY REQUEST para obtener el ID de la solicitud que desea cancelar.</p> <p>Si no responde a la solicitud de dar de alta desde el servidor dentro del periodo de espera de montaje especificado para la clase de dispositivo para la agrupación de almacenamiento, el servidor marcará el volumen como no disponible.</p> |
| Determinar qué volúmenes se montan                                   | Para generar un informe de todos los volúmenes montados actualmente para que los utilice el servidor, emita el mandato QUERY MOUNT. El informe muestra los volúmenes que están montados, las unidades que acceden a ellos y si los volúmenes están en uso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Tarea                           | Detalles                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Desmontar volúmenes desocupados | <p>Cuando un volumen está desocupado, el servidor lo mantiene montado durante un periodo de tiempo especificado por el parámetro de retención de montaje para la clase de dispositivo. El uso de un valor de retención de montaje puede reducir el tiempo de acceso cuando los volúmenes se utilizan reiteradamente.</p> <p>Para desmontar un volumen desocupado desde la unidad donde está montado, emita el mandato DISMOUNT VOLUME.</p> <p>Para obtener información sobre definición de tiempos de retención de montaje, consulte el apartado Control de la cantidad de tiempo que un volumen permanece montado.</p> |

#### Información relacionada:

 QUERY REQUEST (Consultar una o más solicitudes de montaje pendientes)

## Gestión de unidades de cinta

Puede consultar, actualizar y suprimir las unidades de cinta. También puede limpiar las unidades de cinta y configurar el cifrado de unidades de cinta y la validación de datos.

- Actualización de unidades  
Puede cambiar los atributos de una definición de unidad para coger una unidad externa y reconfigurarla.
- Validación de datos durante operaciones de lectura/escritura en cinta  
Para validar datos e identificar los datos dañados, puede utilizar una característica que se llama protección de bloques lógicos. Si utiliza la protección de bloques lógicos, IBM Spectrum Protect inserta un valor de comprobación de redundancia cíclica (CRC) al final de cada bloque lógico de datos cuando se graba en cinta.
- Limpieza de unidades de cinta  
Puede utilizar el servidor para gestionar la limpieza de las unidades de cinta. El servidor puede controlar la limpieza de las unidades de cinta en bibliotecas SCSI.
- Sustitución de unidades de cinta  
Si sustituye una unidad en una biblioteca de cintas definida en IBM Spectrum Protect, debe suprimir las definiciones de unidad y vía de acceso de la unidad antigua y definir la nueva unidad y vía de acceso.

## Actualización de unidades

Puede cambiar los atributos de una definición de unidad para coger una unidad externa y reconfigurarla.

### Acerca de esta tarea

Puede cambiar los siguientes atributos de una unidad.

- La dirección de elemento, si la unidad está en una SCSI
- La frecuencia de limpieza
- El estado de la unidad: en línea o fuera de línea


Restricción: Si una unidad se está utilizando, no se puede cambiar el número de elemento ni el nombre de dispositivo. Para obtener instrucciones sobre cómo externalizar unidades, consulte Poner las unidades de cinta fuera de línea.

Si un volumen está montado en la unidad pero el volumen está desocupado, se puede desmontar explícitamente. Para obtener instrucciones sobre cómo desmontar volúmenes desocupados, consulte Gestión de solicitudes del servidor para los volúmenes.

## Procedimiento

- Cambie la dirección de elemento de una unidad emitiendo el mandato UPDATE DRIVE. Por ejemplo, en una biblioteca denominada AUTO, cambie la dirección de elemento DRIVE3 a 119 emitiendo el mandato siguiente:

```
update drive auto drive3 element=119
```

- Cambie el nombre de dispositivo de una unidad emitiendo el mandato UPDATE PATH. Por ejemplo, para cambiar el nombre de dispositivo de una unidad denominada DRIVE3, emita el mandato siguiente:  Sistemas operativos AIX

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/rmt0
```

 Sistemas operativos Linux

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/IBMtape0
```

#### Sistemas operativos Windows

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=mt3.0.0.0
```

- Poner las unidades de cinta fuera de línea  
Puede poner una unidad de cinta fuera de línea mientras se está utilizando. Por ejemplo, puede poner una unidad de cinta fuera de línea para completar el mantenimiento.

#### Referencia relacionada:

[UPDATE PATH \(Cambiar una vía de acceso\)](#)

#### Información relacionada:

[UPDATE DRIVE \(Actualizar una unidad\)](#)

## Validación de datos durante operaciones de lectura/escritura en cinta

Para validar datos e identificar los datos dañados, puede utilizar una característica que se llama protección de bloques lógicos. Si utiliza la protección de bloques lógicos, IBM Spectrum Protect inserta un valor de comprobación de redundancia cíclica (CRC) al final de cada bloque lógico de datos cuando se graba en cinta.

Con la protección de bloques lógicos, puede identificar los errores que se producen cuando se graban los datos en cinta y durante la transferencia de datos de la unidad de cinta a IBM Spectrum Protect a través de la red de área de almacenamiento. Las unidades que dan soporte a la protección de bloques lógicos validan datos durante las operaciones de lectura y grabación. El servidor de IBM Spectrum Protect valida los datos durante las operaciones de lectura.

Si falla la validación por la unidad durante las operaciones de grabación, la anomalía puede indicar que los datos se han dañado durante la transferencia a cinta. En este caso, el servidor de IBM Spectrum Protect da error en la operación de grabación. Debe reiniciar la operación para continuar. Si falla la validación por la unidad durante las operaciones de lectura, la anomalía puede indicar que el soporte de cinta está dañado. Si falla la validación por el servidor de IBM Spectrum Protect durante las operaciones de lectura, la anomalía puede indicar que los datos se ha dañado durante la transferencia desde la unidad de cinta, y el servidor vuelve a intentar la operación. Si la validación falla constantemente, el servidor de IBM Spectrum Protect emite un mensaje de error que indica problemas de hardware o de conexión.

Si la protección de bloques lógicos está inhabilitada en una unidad de cinta o la unidad no admite la protección de bloques lógicos, el servidor de IBM Spectrum Protect podrá leer los datos protegidos. Sin embargo, los datos no se validan.

La protección de bloques lógicos es superior a la validación de CRC que puede especificar al definir o actualizar una agrupación de almacenamiento. Cuando especifica la validación de CRC para una agrupación de almacenamiento, los datos solo se validarán durante operaciones de auditoría de volumen. Los errores se identifican después de grabar los datos en cinta.

#### Restricciones:

- No puede utilizar la protección de bloques lógicos para datos secuenciales tales como conjuntos de copias de seguridad y copias de seguridad de bases de datos.
- La comprobación CRC afecta al rendimiento porque se necesita más utilización de procesador en el cliente y en el servidor para calcular y comparar valores CRC.
- Para un volumen reutilizable, si especifica la protección de bloque lógico para operaciones de lectura/escritura (LBPROTECT=READWRITE), no cambie el valor del parámetro en cualquier momento después de grabar los datos en el volumen. No se admite cambiar el valor del parámetro durante la vida del volumen en el servidor IBM Spectrum Protect.
- Unidades que dan soporte a la protección de bloques lógicos  
La protección de bloques lógicos solo está disponible para tipos de dispositivo ECARTRIDGE, 3592 y LTO. Las unidades 3592 compatibles incluyen IBM TS1130, TS1140 y generaciones posteriores. Las unidades LTO preparadas incluyen IBM LTO-5 y unidades LTO-6 soportadas. Las unidades Oracle StorageTek compatibles incluyen unidades con el formato T10000C y T10000D.
- Habilitación e inhabilitación de la protección de bloques lógicos  
Puede especificar la protección de bloques lógicos para operaciones de lectura y grabación, o sólo para operaciones de grabación. También puede inhabilitar la protección de bloques lógicos. De forma predeterminada, la protección de bloques lógicos está inhabilitada debido a efectos de rendimiento resultado de la comprobación de redundancia cíclica (CRC) en el servidor y en la unidad de cinta.
- Operaciones de lectura/escritura en volúmenes con protección de bloques lógicos  
Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen.



- Gestión de agrupaciones de almacenamiento en una biblioteca de cintas  
Para mezclar datos protegidos y no protegidos en una biblioteca, debe crear clases de dispositivo y distintas agrupaciones de almacenamiento para separar los datos. Si una clase de dispositivo está asociada a datos protegidos, puede especificar la protección de bloques lógicos para operaciones de lectura y grabación o solo para operaciones de grabación.

## Unidades que dan soporte a la protección de bloques lógicos

La protección de bloques lógicos solo está disponible para tipos de dispositivo ECARTRIDGE, 3592 y LTO. Las unidades 3592 compatibles incluyen IBM TS1130, TS1140 y generaciones posteriores. Las unidades LTO preparadas incluyen IBM LTO-5 y unidades LTO-6 soportadas. Las unidades Oracle StorageTek compatibles incluyen unidades con el formato T10000C y T10000D.

La siguiente tabla muestra los soportes y los formatos que se pueden utilizar con unidades que admitan la protección de bloques lógicos.

| Unidad         | Medio de cinta              | Formatos de unidad             |
|----------------|-----------------------------|--------------------------------|
| IBM TS1130     | 3592 Generación 2           | 3592-3 y 3592-3C               |
| IBM TS1140     | 3592 Generación 2           | Generación 2: 3592-3 y 3592-3C |
|                | 3592 Generación 3           | Generación 3: 3592-4 y 3592-4C |
| IBM TS1150     | 3592 Generación 3           | Generación 4: 3592-5 y 3592-5C |
|                | 3592 Generación 4           |                                |
| IBM LTO-5      | LTO-5                       | Ultrium 5 y Ultrium 5C         |
| IBM LTO-6      | LTO-6                       | Ultrium 6 y Ultrium 6C         |
|                | LTO-5                       | Ultrium 5 y Ultrium 5C         |
| IBM LTO-7      | LTO-7                       | Ultrium 7 y Ultrium 7C         |
|                | LTO-6                       | Ultrium 6 y Ultrium 6C         |
| Oracle T10000C | Oracle StorageTek T10000 T2 | T10000C y T10000C-C            |
| Oracle T10000D | Oracle StorageTek T10000 T2 | T10000D y T10000D-C            |

Sugerencias:

- Para habilitar la protección de bloques lógicos para un volumen de cinta y después reutilizar el volumen para hacer una copia de seguridad de los datos, debe habilitar la protección de bloques lógicos para esa clase de dispositivo y para la unidad.
- Si tiene una unidad 3592, LTO, u Oracle StorageTek que no permite protección de bloques lógicos, puede actualizar la unidad con firmware que proporcione protección de bloques lógicos.

La protección de bloques lógicos está disponible para unidades que estén en SCSI bibliotecas. Para obtener la información más actual sobre el soporte para la protección de bloques lógicos, consulte la nota técnica 1568108.

Para utilizar la protección de bloques lógicos para operaciones de grabación, todas las unidades de la biblioteca deben admitir este tipo de protección. Si una unidad no permite la protección de bloques lógicos, no se montarán los volúmenes que tengan acceso de lectura y grabación. No obstante, el servidor puede utilizar la unidad para montar volúmenes que tengan acceso de sólo lectura. El servidor de IBM Spectrum Protect lee y valida los datos protegidos si la protección de bloques lógicos está habilitada para las operaciones de lectura/escritura.

## Habilitación e inhabilitación de la protección de bloques lógicos

Puede especificar la protección de bloques lógicos para operaciones de lectura y grabación, o sólo para operaciones de grabación. También puede inhabilitar la protección de bloques lógicos. De forma predeterminada, la protección de bloques lógicos está inhabilitada debido a efectos de rendimiento resultado de la comprobación de redundancia cíclica (CRC) en el servidor y en la unidad de cinta.

### Acerca de esta tarea

Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen. Si cambia el valor de la protección de bloques lógicos, el cambio solo se aplica a los volúmenes vacíos. Los volúmenes que ya están llenos o los que se están llenando mantienen su estado de protección de bloques lógicos hasta que están vacíos y listos para ser llenados de nuevo. Por

ejemplo, si inhabilita la protección de bloques lógicos y el servidor selecciona un volumen que está asociado con una clase de dispositivo que tiene protección de bloques lógicos, el servidor sigue grabando datos protegidos en el volumen.

Restricción: La protección de bloques lógicos solo está disponible para ciertos tipos de dispositivo. Para obtener más información, consulte Unidades que dan soporte a la protección de bloques lógicos.

## Procedimiento

---

1. Para habilitar la protección de bloques lógicos para tipos de dispositivo 3592, LTO y ECARTRIDGE, emita el mandato DEFINE DEVCLASS o UPDATE DEVCLASS y especifique el parámetro LBPROTECT. Por ejemplo, para especificar la protección de bloques lógicos durante las operaciones de lectura y escritura para una clase de dispositivo 3592 denominada 3592\_lbprotect, emita el mandato siguiente:

```
define devclass 3592_lbprotect library=3594 lbprotect=readwrite
```

Sugerencias:

- Si actualiza el valor del parámetro LBPROTECT de NO a READWRITE o WRITEONLY y el servidor selecciona un volumen de relleno sin protección de bloque lógico para las operaciones de grabación, el servidor emite un mensaje cada vez que se monta el volumen. El mensaje indica que los datos se grabarán en el volumen sin protección de bloque lógico. Para evitar que aparezca este mensaje o para que IBM Spectrum Protect solo grabe datos sin protección de bloque lógico, actualice el acceso de los volúmenes de relleno sin protección de bloque lógico a de solo lectura.
  - Para mejorar el rendimiento, no especifique el parámetro CRCDATA en el mandato DEFINE STGPOOL ni en el mandato UPDATE STGPOOL.
  - Cuando se validan los datos durante las operaciones de lectura, tanto por parte de la unidad como del servidor de IBM Spectrum Protect, puede ralentizar el rendimiento del servidor durante las operaciones de restauración y recuperación. Para reducir el tiempo necesario para las operaciones de restauración y recuperación, cambie el valor del parámetro LBPROTECT de READWRITE a WRITEONLY. Una vez restaurados o recuperados los datos, puede restablecer el parámetro LBPROTECT en READWRITE.
2. Para inhabilitar la protección de bloques lógicos, emita el mandato DEFINE DEVCLASS o el mandato UPDATE DEVCLASS y especifique el parámetro LBPROTECT=NO.

Restricción: Si la protección de bloques lógicos está inhabilitada, el servidor no graba en una cinta vacía con protección de bloques lógicos. No obstante, si se selecciona un volumen de relleno con protección de bloques lógicos, el servidor sigue grabando en el volumen con protección de bloques lógicos. Para impedir que el servidor grabe en cintas con protección de bloques lógicos, cambie el acceso de los volúmenes de relleno con protección de bloques lógicos a de sólo lectura. Cuando se leen los datos, la unidad o el servidor no comprueban los resultados de la CRC.

Si se produce un siniestro y el sitio de recuperación tras desastre no tiene unidades que admitan protección de bloques lógicos, debe especificar el parámetro LBPROTECT=NO. Si las unidades de cinta se utilizan para operaciones de grabación, deberá cambiar el acceso de volumen para los volúmenes con datos protegidos a "sólo lectura" para impedir que el servidor utilice los volúmenes.

Si el servidor debe habilitar la protección de bloques lógicos, el servidor emite un mensaje de error indicando que la unidad no admite protección de bloques lógicos.

## Qué hacer a continuación

---

Para determinar si un volumen tiene protección de bloques lógicos, emita el mandato QUERY VOLUME y revise el valor del campo Logical Block Protection.

### Referencia relacionada:

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

### Información relacionada:

- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)
- ➔ QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Operaciones de lectura/escritura en volúmenes con protección de bloques lógicos

---

Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen.

Si utiliza el mandato UPDATE DEVCLASS para cambiar el valor de la protección de bloques lógicos, el cambio solo se aplica a los volúmenes vacíos. Los volúmenes que ya están llenos o los que se están llenando mantienen su estado de protección de bloques lógicos hasta que están vacíos y listos para ser llenados de nuevo.

Por ejemplo, supongamos que cambia el valor del parámetro LBPROTECT de READWRITE a NO. Si el servidor selecciona un volumen que está asociado con la clase de dispositivo que tiene la protección de bloques lógicos, el servidor sigue grabando datos protegidos en el volumen.

Sugerencias:

- Si una unidad no admite la protección de bloques lógicos, no se pueden montar los volúmenes con protección de bloques lógicos para las operaciones de grabación. Para evitar que el servidor monte volúmenes protegidos para operaciones de grabación, cambie el acceso del volumen a sólo lectura. Además, inhabilite la protección de bloques lógicos para impedir que el servidor habilite la función en la unidad de cintas.
- Si una unidad no admite la protección de bloques lógicos, y la protección de bloques lógicos se inhabilita, el servidor lee los datos de los volúmenes protegidos. No obstante, ni servidor ni la unidad de cintas validan los datos.

**Información relacionada:**

- QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Gestión de agrupaciones de almacenamiento en una biblioteca de cintas

---

Para mezclar datos protegidos y no protegidos en una biblioteca, debe crear clases de dispositivo y distintas agrupaciones de almacenamiento para separar los datos. Si una clase de dispositivo está asociada a datos protegidos, puede especificar la protección de bloques lógicos para operaciones de lectura y grabación o solo para operaciones de grabación.

Para definir clases de dispositivos y agrupaciones de almacenamiento para una biblioteca TS3500 que tiene unidades LTO-5, para datos protegidos y no protegidos, puede emitir una serie de mandatos como se muestra en el ejemplo siguiente:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

**Referencia relacionada:**

- DEFINE DEVCLASS (Definir una clase de dispositivo)

**Información relacionada:**

- DEFINE LIBRARY (Definir una biblioteca)
- DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Limpieza de unidades de cinta

---

Puede utilizar el servidor para gestionar la limpieza de las unidades de cinta. El servidor puede controlar la limpieza de las unidades de cinta en bibliotecas SCSI.

### Acerca de esta tarea

---

Debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones para poder limpiar unidades de cinta. Para las bibliotecas automatizadas, puede automatizar la limpieza especificando la frecuencia de las operaciones de limpieza y comprobando que haya un cartucho limpiador en el inventario de volúmenes de la biblioteca. IBM Spectrum Protect monta el cartucho limpiador tal y como se especifica. Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades controladas por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

Consejo: Si una biblioteca de cintas automatizada admite la limpieza de las unidades de la biblioteca, asegúrese de que la característica está habilitada.

Puede prevenir el desgaste prematuro de los cabezales de lectura/escritura de las unidades utilizando las funciones de limpieza de biblioteca que proporciona el fabricante del dispositivo.

Las unidades y las bibliotecas de fabricantes distintos se distinguen entre sí en la forma de gestionar los cartuchos limpiadores y en cómo informan de la presencia de un cartucho limpiador en una unidad. Es posible que el controlador de dispositivo no pueda abrir la unidad que contiene el cartucho limpiador. Los códigos de detección y de error que emiten los dispositivos para la limpieza de unidades

son variados. La limpieza de unidades de la biblioteca normalmente es desconocida para las aplicaciones. Así pues, es posible que IBM Spectrum Protect no siempre detecte los cartuchos limpiadores en las unidades y puede que no sea capaz de determinar cuando empieza la limpieza.

Algunos dispositivos necesitan un cierto tiempo de inactividad entre solicitudes de montaje para iniciar la limpieza de unidades. Sin embargo, IBM Spectrum Protect intenta minimizar el tiempo de inactividad para una unidad. Esto puede suponer que se impida el buen funcionamiento de la limpieza de unidades de la biblioteca. Si esto sucediera, intente utilizar IBM Spectrum Protect para controlar la limpieza de unidades. Puede establecer la frecuencia de forma que coincida con las recomendaciones de limpieza del fabricante.

- **Métodos para limpiar unidades de cinta**  
Con el tiempo, los cabezales de lectura de las cintas pueden ensuciarse, lo que puede hacer que fallen las operaciones de lectura y grabación. Para evitar estos problemas, habilite la limpieza de cintas. Puede habilitar la limpieza de cintas de la unidad o desde IBM Spectrum Protect.
- **Configuración del servidor para la limpieza de unidades en una biblioteca automatizada**  
Al configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, puede especificar la frecuencia con la que desea que se limpien las unidades.
- **Resolución de errores relacionados con la limpieza de unidades**  
Al mover cartuchos dentro de una biblioteca, puede que coloque un cartucho de datos donde debería ir un cartucho limpiador. Revise el proceso que ha completado el servidor y los mensajes que se han emitido para resolver el problema.

## Métodos para limpiar unidades de cinta

---

Con el tiempo, los cabezales de lectura de las cintas pueden ensuciarse, lo que puede hacer que fallen las operaciones de lectura y grabación. Para evitar estos problemas, habilite la limpieza de cintas. Puede habilitar la limpieza de cintas de la unidad o desde IBM Spectrum Protect.

Puede elegir utilizar el método de limpieza de unidades de biblioteca o el método de limpieza de unidades de IBM Spectrum Protect, pero no ambos. Algunas bibliotecas SCSI proporcionan la limpieza automática de las unidades. Seleccione el método de limpieza de unidades de biblioteca si está disponible. Si no está disponible o da problemas, utilice IBM Spectrum Protect para controlar la limpieza de unidades de biblioteca.

### Método de limpieza de unidades de biblioteca

El método de limpieza de unidades de biblioteca proporciona varias ventajas para las bibliotecas de cintas automatizadas que utilizan esta función.

- Reduce la carga sobre el administrador de IBM Spectrum Protect de gestionar físicamente la limpieza de los cartuchos.
- Mejora las tasas de uso del cartucho de limpieza. La mayoría de bibliotecas de cintas hacen un seguimiento del número de veces que se pueden limpiar las unidades basándose en los indicadores de hardware. IBM Spectrum Protect utiliza un recuento bruto.
- Reduce las limpiezas innecesarias. Las unidades de cinta modernas no se tienen que limpiar a intervalos fijos, pueden detectar y solicitar cuándo necesitan una limpieza.

Los fabricantes que proporcionan un método de limpieza de unidades de biblioteca, recomiendan utilizarlo para evitar un desgaste prematuro de los cabezales de lectura/escritura de las unidades. Las unidades y las bibliotecas de fabricantes distintos se distinguen entre sí en la forma de gestionar los cartuchos limpiadores y en cómo informan de la presencia de un cartucho limpiador en una unidad. Es posible que el controlador de dispositivo no pueda abrir la unidad que contiene el cartucho limpiador. Los códigos de detección y de error que emiten los dispositivos para la limpieza de unidades son variados. La limpieza de unidades de biblioteca normalmente es transparente para todas las aplicaciones. No obstante, es posible que IBM Spectrum Protect no siempre detecte los cartuchos limpiadores en las unidades y puede que no sea capaz de determinar cuando empieza la limpieza.

### Método de limpieza de unidades de IBM Spectrum Protect

Algunos dispositivos necesitan un cierto tiempo de inactividad entre solicitudes de montaje para iniciar la limpieza de unidades. Sin embargo, IBM Spectrum Protect intenta minimizar el tiempo de inactividad para una unidad. Esto puede suponer que se impida el buen funcionamiento de la limpieza de unidades de la biblioteca. Si esto sucediera, intente utilizar IBM Spectrum Protect para controlar la limpieza de unidades. Establezca la frecuencia de forma que coincida con las recomendaciones de limpieza del fabricante.

Si IBM Spectrum Protect controla el proceso de limpieza de unidades, inhabilite la función de limpieza de unidades de biblioteca para evitar problemas. Si la función de limpieza de unidades de biblioteca está habilitada, algunos dispositivos mueven automáticamente cualquier cartucho limpiador que encuentren en la biblioteca a ranuras de la biblioteca dedicadas a cartuchos limpiadores. No podrá dar de alta un cartucho limpiador en el inventario de biblioteca de IBM Spectrum Protect hasta que inhabilite la función de limpieza de unidades de biblioteca.

Para habilitar la limpieza desde la unidad, siga las instrucciones proporcionadas por el fabricante de la misma. Para habilitar la limpieza utilizando IBM Spectrum Protect, consulte Configuración del servidor para la limpieza de unidades en una biblioteca automatizada.

## Configuración del servidor para la limpieza de unidades en una biblioteca automatizada

---

Al configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, puede especificar la frecuencia con la que desea que se limpien las unidades.

### Antes de empezar




---

Determine la frecuencia con la que se debe limpiar la unidad. Este paso es necesario para que pueda especificar el valor adecuado para el parámetro CLEANFREQUENCY en el mandato DEFINE DRIVE o UPDATE DRIVE. Por ejemplo, para limpiar una unidad tras procesar 100 GB de datos en la misma, tendría que especificar CLEANFREQUENCY=100.

Para obtener directrices sobre la frecuencia de limpieza, consulte la documentación del fabricante de la unidad. Si la documentación proporciona directrices para la frecuencia de limpieza en términos de horas de uso, puede convertir el valor en un valor en gigabytes completando los pasos siguientes :

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor de gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.

Puede especificar un valor para el parámetro CLEANFREQUENCY o especificar ASNEEDED para limpiar la unidad según sea necesario. Restricciones:

1. Para unidades IBM® 3592, debe especificar un valor numérico para el parámetro CLEANFREQUENCY. Si utiliza la frecuencia de limpieza que se indica en la documentación del producto, no limpiará las unidades más de la cuenta.
2. El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Para determinar si una unidad admite esta función, consulte la información de su sistema operativo.
  -  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos soportados para AIX y Windows
  -  Sistemas operativos Linux Dispositivos soportados para Linux

En la nota técnica, pulse en el nombre de la unidad para ver la información detallada. SI el valor ASNEEDED no está soportado, especifique el número de gigabytes.

### Procedimiento

---

Para configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, complete los pasos siguientes:

Defina o actualice las unidades en la biblioteca utilizando el parámetro CLEANFREQUENCY en el mandato DEFINE DRIVE o UPDATE DRIVE. Por ejemplo, para limpiar una unidad denominada DRIVE1 tras procesar 100 GB de datos, emita el mandato siguiente:

```
update drive autolib1 drive1 cleanfrequency=100
```

### Resultados

---

Una vez que el cartucho limpiador esté dado de alta, el servidor montará el cartucho limpiador en una unidad cuando ésta necesite limpieza. El servidor utiliza ese cartucho para el número de limpiezas especificado. Para obtener más información, consulte Operaciones con cartuchos limpiadores.

### Qué hacer a continuación

---

Incorpore el cartucho limpiador en el inventario de volúmenes de biblioteca siguiendo las instrucciones que encontrará en Incorporar un cartucho limpiador en una biblioteca.

- Incorporar un cartucho limpiador en una biblioteca  
Para habilitar la limpieza automática de unidades de cinta, debe incorporar un cartucho limpiador en el inventario de volúmenes de la biblioteca automatizada.
- Operaciones con cartuchos limpiadores  
Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

**Información relacionada:**

- ➔ DEFINE DRIVE (Definir una unidad en una biblioteca)
- ➔ UPDATE DRIVE (Actualizar una unidad)

## Incorporar un cartucho limpiador en una biblioteca

---

Para habilitar la limpieza automática de unidades de cinta, debe incorporar un cartucho limpiador en el inventario de volúmenes de la biblioteca automatizada.

### Acerca de esta tarea

---

Al incorporar un cartucho limpiador a una biblioteca, asegúrese de que está correctamente identificado en el servidor como cartucho limpiador. Asegúrese de que el cartucho limpiador no se encuentre en una ranura que pueda detectar un proceso de búsqueda. Si se producen errores o retrasos de 15 minutos o más, puede ser indicativo de que hay un cartucho limpiador mal colocado.

El método preferido es dar de alta los cartuchos limpiadores individualmente. Si tiene que dar de alta cartuchos de datos y cartuchos limpiadores, ponga los cartuchos de datos en la biblioteca e incorpórelos antes. A continuación incorpore el cartucho limpiador a la biblioteca.

### Procedimiento

---

Para incorporar un cartucho limpiador a una biblioteca, emita el mandato CHECKIN LIBVOLUME. Por ejemplo, para dar de alta un cartucho limpiador denominado AUTOLIB1, emita el mandato siguiente:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10
checklabel=no
```

El servidor solicita que el cartucho se coloque en el puerto de entrada/salida o en una ranura específica.

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

## Operaciones con cartuchos limpiadores

---

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

**Supervisión del proceso de limpieza**

Si se ha incorporado un cartucho limpiador en una biblioteca y se tiene que limpiar una unidad, el servidor desmonta el volumen de datos y ejecuta la operación de limpieza. Si la operación de limpieza falla o se cancela, o si no hay ningún cartucho limpiador disponible, puede que no se dé cuenta de que la unidad necesita una limpieza. Supervise los mensajes sobre estos problemas de limpieza para asegurarse de que las unidades se limpian cuando es necesario. Si es necesario, emita el mandato CLEAN DRIVE para que el servidor intente la limpieza de nuevo, o cargue manualmente un cartucho limpiador en la unidad.

**Utilización de varios cartuchos limpiadores**

El servidor utiliza un cartucho limpiador para el número de limpiezas que especifique al dar de alta el cartucho limpiador. Si incorpora dos o más cartuchos limpiadores, el servidor utilizará sólo uno de los cartuchos hasta alcanzar el número de limpiezas designado para ese cartucho. A continuación, el servidor utiliza el siguiente cartucho limpiador. Si incorpora dos o más cartuchos limpiadores y ejecuta simultáneamente dos o más mandatos CLEAN DRIVE, el servidor utilizará varios cartuchos al mismo tiempo y reducirá las limpiezas restantes en cada cartucho.

**Referencia relacionada:**

- ➔ AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ CLEAN DRIVE (Limpiar una unidad)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)

**Información relacionada:**

- ➔ QUERY LIBVOLUME (Consultar un volumen de biblioteca)

## Resolución de errores relacionados con la limpieza de unidades

---

Al mover cartuchos dentro de una biblioteca, puede que coloque un cartucho de datos donde debería ir un cartucho limpiador. Revise el proceso que ha completado el servidor y los mensajes que se han emitido para resolver el problema.

Cuando una unidad necesita una limpieza, el servidor carga el cartucho que en su base de datos se indica como cartucho limpiador en la unidad. A continuación, la unidad pasa al estado READY y IBM Spectrum Protect detecta que el cartucho es un cartucho de datos. El servidor completa los pasos siguientes:

1. El servidor intenta leer la etiqueta de la cinta interna del cartucho de datos.
2. El servidor expulsa el cartucho de la unidad y lo mueve a la ranura inicial del cartucho limpiador dentro de la biblioteca. Si la operación de expulsión falla, el servidor marca la unidad como fuera de línea y emite un mensaje indicando que el cartucho todavía se encuentra en la unidad.
3. El servidor extrae el cartucho limpiador para evitar seleccionarlo para otra solicitud de limpieza de la unidad. El cartucho limpiador permanece en la biblioteca pero ya no aparece en el inventario de biblioteca de IBM Spectrum Protect.
4. Utilizando la etiqueta de cinta interna, el servidor comprueba el nombre del volumen en el inventario de biblioteca actual, los volúmenes de agrupación de almacenamiento y el archivo de historial de volúmenes.
  - Si el nombre del volumen no se encuentra en el inventario de la biblioteca, puede que se haya dado de alta un cartucho de datos como cartucho limpiador por error. Una vez extraído el volumen, no tiene que hacer nada más.
  - Si el nombre del volumen se encuentra en el inventario de la biblioteca, el servidor emite mensajes de que se requiere una intervención manual y una auditoría de biblioteca. Para resolver este problema, siga las instrucciones de Auditoría de inventarios de volúmenes en una biblioteca.

## Sustitución de unidades de cinta

---

Si sustituye una unidad en una biblioteca de cintas definida en IBM Spectrum Protect, debe suprimir las definiciones de unidad y vía de acceso de la unidad antigua y definir la nueva unidad y vía de acceso.

La sustitución de definiciones de unidad y vía de acceso es necesaria aunque esté intercambiando una unidad por otra del mismo tipo, utilizando la misma dirección lógica y dirección física, el mismo ID de SCSI y el mismo número de puerto. Los nombres de alias de dispositivo se pueden cambiar cuando se cambian las conexiones de las unidades.

Si la unidad nueva es una actualización que da soporte a un nuevo formato de medios, es posible que también tenga que definir una nueva biblioteca lógica, clase de dispositivo y agrupación de almacenamiento. Los procedimientos para configurar una política para una nueva unidad en una biblioteca de múltiples unidades varían según los tipos de unidades y medios que haya en la biblioteca.

- Suprimir unidades de cinta  
Puede suprimir unidades de cinta de una biblioteca. Por ejemplo, puede suprimir una unidad que ya no utilice o que desee sustituir.
- Sustitución de las unidades con otras del mismo tipo  
Para añadir una unidad que admita los mismos formatos de medios que la unidad a la que sustituye, debe definir una unidad y una vía de acceso nuevas.
- Migración de datos a unidades actualizadas  
Su actualiza todas las unidades de cinta de una biblioteca, puede conservar las definiciones de política existente para migrar y caducar los datos existentes, y puede utilizar las nuevas unidades para almacenar datos.

## Suprimir unidades de cinta

---

Puede suprimir unidades de cinta de una biblioteca. Por ejemplo, puede suprimir una unidad que ya no utilice o que desee sustituir.

### Procedimiento

---

1. Detenga el servidor de IBM Spectrum Protect y cierre el sistema operativo.
2. Extraiga la unidad antigua y siga las instrucciones del fabricante para instalar la unidad nueva.
3. Reinicie el sistema operativo y el servidor de IBM Spectrum Protect.
4. Suprima la vía de acceso desde el servidor a la unidad. Por ejemplo, para suprimir una vía de acceso de SERVER1 a LIB1, emita el mandato siguiente:

```
delete path server1 lib1 srctype=server desttype=drive
```

5. Suprima la definición de la unidad. Por ejemplo, emita el siguiente mandato para suprimir una unidad denominada DLT1 de un dispositivo de biblioteca denominado LIB1:

```
delete drive lib1 dlt1
```

#### Referencia relacionada:

- [DELETEDRIVE \(Suprimir una unidad de una biblioteca\)](#)
- [DELETEPATH \(suprimir una vía de acceso\)](#)

## Sustitución de las unidades con otras del mismo tipo

---

Para añadir una unidad que admita los mismos formatos de medios que la unidad a la que sustituye, debe definir una unidad y una vía de acceso nuevas.

### Acerca de esta tarea

---

Si una biblioteca sólo incluye un modelo de unidad y desea sustituir una unidad, debe sustituir la unidad por la misma unidad de modelo. Si una biblioteca incluye modelos mixtos de unidades y usted desea sustituir una unidad, puede sustituir el modelo por cualquier unidad de modelo que exista en la biblioteca.


### Procedimiento

---

1. Suprima la vía de acceso y las definiciones de unidad de la unidad antigua. Por ejemplo, para suprimir una unidad denominada DRIVE1 de una biblioteca denominada LIB1, emita el mandato siguiente:

```
delete path server2 drive1 srctype=server desttype=drive library=lib1
delete drive lib1 drive1
```

2. Apague la biblioteca, elimine la unidad original, sustitúyala por la nueva unidad y encienda la biblioteca.
3. Actualice el sistema host para asegurarse de que el sistema detecta la nueva unidad.
4. Defina la unidad y la vía de acceso nuevas. Por ejemplo, para definir una nueva unidad, DRIVE2, y una vía de acceso a ella desde SERVER2, si utiliza un controlador de dispositivo IBM Spectrum Protect, escriba los siguientes mandatos:

 Sistemas operativos AIX

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/mt0
```

 Sistemas operativos Linux



```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/tmscsi/mt0
```

 Sistemas operativos Windows

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=mt3.0.0.1
```

Consejo: Puede utilizar las definiciones de biblioteca, clase de dispositivo y agrupación de almacenamiento existentes.

#### Referencia relacionada:

-  [DELETE DRIVE \(Suprimir una unidad de una biblioteca\)](#)
-  [DELETE PATH \(suprimir una vía de acceso\)](#)

## Migración de datos a unidades actualizadas

---

Su actualiza todas las unidades de cinta de una biblioteca, puede conservar las definiciones de política existente para migrar y caducar los datos existentes, y puede utilizar las nuevas unidades para almacenar datos.

### Antes de empezar

---

En el ejemplo siguiente se presupone que ya dispone de una agrupación de almacenamiento primario para una clase de dispositivo DISK denominada POOL1.

### Procedimiento

---

1. Para migrar los datos a una agrupación de almacenamiento que se haya creado para las nuevas unidades, especifique el parámetro NEXTSTGPOOL. Por ejemplo, para migrar datos de una agrupación de almacenamiento existente, POOL1, a la nueva agrupación de almacenamiento, POOL2, emita el mandato siguiente:

```
update stgpool pool1 nextstgpool=pool2
```



- Actualice las definiciones de clase de gestión existentes para almacenar datos en la agrupación de almacenamiento DISK utilizando el mandato UPDATE MGMTCLASS.

**Referencia relacionada:**

- ➔ UPDATE MGMTCLASS (Actualizar una clase de gestión)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

**Información relacionada:**

- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Protección del servidor IBM Spectrum Protect

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- **Gestión de administradores**  
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.
- **Cambio de los requisitos de contraseña**  
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- **Protección del servidor en el sistema**  
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

## Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

### Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

| Tarea                                  | Procedimiento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Añada un administrador.                | <p>Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:</p> <ol style="list-style-type: none"> <li>Registre el administrador y especifique Pa\$\$twO como contraseña ejecutando el siguiente mandato:<br/><code>register admin admin1 Pa\$\$twO</code></li> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:<br/><code>grant authority admin1 classes=system</code></li> </ol> |
| Cambie los permisos del administrador. | <p>Cambie el nivel de autorización de un administrador, ADMIN1.</p> <ul style="list-style-type: none"> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:<br/><code>grant authority admin1 classes=system</code></li> <li>Emita el siguiente mandato para revocar la autoridad del sistema del administrador:<br/><code>revoke authority admin1 classes=system</code></li> </ul>                                                                     |
| Elimine administradores.               | <p>Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect:<br/><code>remove admin admin1</code></p>                                                                                                                                                                                                                                                                                                                             |

| Tarea                                           | Procedimiento                                                                                |
|-------------------------------------------------|----------------------------------------------------------------------------------------------|
| Impida el acceso al servidor de forma temporal. | Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador. |

**Conceptos relacionados:**

Planificación de los roles de administración

## Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

### Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

### Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

| Tarea                                                      | Procedimiento                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establecer un límite de intentos de contraseña no válidos. | <ul style="list-style-type: none"> <li>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>b. Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</li> <li>c. Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</li> </ul> <p>El valor predeterminado en la instalación es 0.</p>                                                   |
| Establezca una longitud mínima para las contraseñas.       | <ul style="list-style-type: none"> <li>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>c. Establezca el número de caracteres en el campo Longitud de contraseña mínima.</li> </ul>                                                                                                                                              |
| Establezca el periodo de caducidad para las contraseñas.   | <ul style="list-style-type: none"> <li>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>c. Establecer el número de días en el campo Caducidad común de la contraseña.</li> </ul>                                                                                                                                                 |
| Inhabilitar la autenticación de contraseña.                | <p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.</p> <p>Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.</p> |

| Tarea                                                 | Procedimiento                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establecer un método de autenticación predeterminado. | <p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre> |

## Protección del servidor en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

### Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor  
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

## Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

### Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- Detención del servidor  
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- Inicio del servidor para tareas de mantenimiento o reconfiguración  
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Detención del servidor

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

### Acerca de esta tarea

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

### Procedimiento

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:

- a. En la página Visión general del Centro de operaciones, vea el área Actividad para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.

b. Vea el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:

- El periodo actual, es decir, el periodo de 24 horas más reciente
- El periodo anterior, es decir, 24 horas antes del periodo actual

Si el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.

- c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.

3. Espere hasta que las sesiones de nodo cliente se completen o cancélelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:

- En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
- Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
- Pulse Cancelar.
- Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.  
Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.

4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

## Inicio del servidor para tareas de mantenimiento o reconfiguración

---

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, dsmserv.opt, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

### Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.




## Qué hacer a continuación

---

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
  -  Sistemas operativos AIX Inicio de la instancia de servidor
  -  Sistemas operativos Linux Inicio de la instancia de servidor
  -  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

## Planificación para actualizar el servidor

---

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

### Acerca de esta tarea

---

Siga estas directrices:

- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

### Procedimiento




---

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.  
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

## Qué hacer a continuación

---

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

#### Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

## Preparación para una parada o actualización de sistema

---

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

### Acerca de esta tarea

---

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor. Para obtener información acerca de la planificación actividades como la copia de seguridad de la base de datos, la copia de seguridad del archivo de configuración de dispositivo, y la copia de seguridad del historial de volumen, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

## Procedimiento

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
  - a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
  - b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - c. Pulse Cancelar.
2. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

### Referencia relacionada:

[HALT \(Concluir el servidor\)](#)

## Preparación ante desastres y recuperación tras desastres mediante DRM

IBM Spectrum Protect proporciona una función de gestor recuperación tras desastre (DRM) para poder recuperar los datos del servidor y del cliente durante un siniestro.

DRM realiza el seguimiento del movimiento de los medios fuera del sitio y registra esa información en la base de datos de IBM Spectrum Protect. DRM consolida los planes, los scripts y cualquier otra información de un archivo de plan que sea necesaria para recuperar el servidor de IBM Spectrum Protect cuando se produce un siniestro o una parada no prevista del sistema. Si le preocupan los posibles ataques de malware, entre ellos ransomware, considere utilizar DRM, ya que puede ayudarle a recuperar los servidores después de que se haya producido un ataque.

Restricción: DRM solo está disponible en el producto IBM Spectrum Protect Extended Edition.

- Archivo del plan de recuperación tras desastre  
El archivo del plan de recuperación tras desastre contiene la información que se necesita para recuperar un servidor de IBM Spectrum Protect al punto en el tiempo de la última operación de copia de seguridad de la base de datos antes de crear el plan.
- Recuperación de datos de cliente y servidor utilizando DRM  
Utilice la función gestor recuperación tras desastre (DRM) para recuperar el servidor de IBM Spectrum Protect y los datos de cliente cuando se produzca un siniestro.
- Ejecución de obtenciones de detalles de recuperación tras desastre  
Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.
- Restauración de la base de datos  
Si tiene habilitada la función gestor recuperación tras desastre (DRM) y ha seguido el procedimiento para prepararse ante un desastre, puede restaurar la base de datos después de que se produzca un desastre. Si no tiene configurado DRM, todavía podrá restaurar la base de datos, siempre que tenga los archivos de copia de seguridad necesarios.

## Archivo del plan de recuperación tras desastre

El archivo del plan de recuperación tras desastre contiene la información que se necesita para recuperar un servidor de IBM Spectrum Protect al punto en el tiempo de la última operación de copia de seguridad de la base de datos antes de crear el plan.

El plan se organiza en secciones, que puede separar en diversos archivos. Cada sección tiene una sentencia de inicio y una sentencia de finalización.

Tabla 1. Secciones del archivo del plan de recuperación tras desastre

| Sección             | Información de la sección                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------|
| SERVER.REQUIREMENTS | Identifica los requisitos de almacenamiento de la base de datos y del registro de recuperación para el servidor. |

| Sección                                | Información de la sección                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RECOVERY.INSTRUCTIONS.GENERAL          | Identifica las instrucciones específicas del sitio que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.GENERAL. En las instrucciones se incluye la estrategia de recuperación, los nombres de contacto clave, una visión general de las aplicaciones clave de las que este servidor hace copia de seguridad y otras instrucciones de recuperación relevantes.                                     |
| RECOVERY.INSTRUCTIONS.OFFSITE          | Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.OFFSITE. En las instrucciones se describe el nombre y la ubicación de la caja fuerte externa y cómo ponerse en contacto con el administrador de la caja fuerte (por ejemplo, un nombre y un número de teléfono) .                                                                                                      |
| RECOVERY.INSTRUCTIONS.INSTALL          | Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.INSTALL. En las instrucciones se describe cómo reconstruir el servidor base y se proporciona la ubicación de las copias de seguridad de la imagen del sistema.                                                                                                                                                         |
| RECOVERY.INSTRUCTIONS.DATABASE         | Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.DATABASE. En las instrucciones se describe cómo preparar la recuperación de la base de datos. Por ejemplo, puede especificar instrucciones sobre cómo inicializar o cargar los volúmenes de copia de seguridad de una biblioteca automatizada. No se proporciona ningún ejemplo de esta sección.                       |
| RECOVERY.INSTRUCTIONS.STGPOOL          | Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.STGPOOL. En las instrucciones se incluyen los nombres de sus aplicaciones de software y los nombres de las agrupaciones de almacenamiento de copias que contienen las copias de seguridad de estas aplicaciones. No se proporciona ningún ejemplo de esta sección.                                                     |
| RECOVERY.VOLUMES.REQUIRED              | Proporciona una lista de volúmenes de copia de seguridad de base de datos y volúmenes de agrupación de almacenamiento de copias necesarios para recuperar el servidor. Se incluye un volumen de copia de seguridad de la base de datos incluye si forma parte de la serie más reciente de copia de seguridad de la base de datos. Un volumen de la agrupación de almacenamiento de copia se incluye si no está vacío y no está marcado como destruido. |
| RECOVERY.DEVICES.REQUIRED              | Proporciona detalles sobre los dispositivos necesarios para leer los volúmenes de copia de seguridad.                                                                                                                                                                                                                                                                                                                                                  |
| RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE | Contiene un script con los mandatos necesarios para recuperar el servidor.                                                                                                                                                                                                                                                                                                                                                                             |
| RECOVERY.SCRIPT.NORMAL.MODE            | Contiene un script con los mandatos necesarios para restaurar las agrupaciones de almacenamiento primarias del servidor.                                                                                                                                                                                                                                                                                                                               |
| DB.STORAGEPATHS                        | Identifica los directorios de la base de datos de IBM Spectrum Protect.                                                                                                                                                                                                                                                                                                                                                                                |
| LICENSE.REGISTRATION                   | Contiene una macro para registrar licencias de su servidor.                                                                                                                                                                                                                                                                                                                                                                                            |
| COPYSTGPOOL.VOLUMES.AVAILABLE          | Contiene una macro para marcar los volúmenes de agrupación de almacenamiento de copias que se han movido fuera del sitio y después se han devuelto al sitio. Puede utilizar la información como guía y ejecutar los mandatos administrativos. Como alternativa, puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                      |

| Sección                       | Información de la sección                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| COPYSTGPOOL.VOLUMES.DESTROYED | Contiene una macro para marcar los volúmenes de agrupación de almacenamiento de copias como no disponibles si los volúmenes estaban en el local en el momento de producirse el siniestro. Se considera que estos volúmenes están fuera del local y, por consiguiente, no han sido destruidos en un siniestro. Puede utilizar la información como guía y emitir los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE. |
| PRIMARY.VOLUMES.DESTROYED     | Contiene una macro para marcar los volúmenes de agrupación de almacenamiento primario como destruidos si los volúmenes estaban en el sitio en el momento de producirse el siniestro. Puede utilizar la información como guía y ejecutar los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                                                                                        |
| PRIMARY.VOLUMES.REPLACEMENT   | Contiene una macro para identificar los volúmenes de agrupación de almacenamiento primaria de sustitución. Puede utilizar la información como guía y ejecutar los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                                                                                                                                                                  |
| STGPOOLS.RESTORE              | Contiene una macro para restaurar las agrupaciones de almacenamiento primarias. Puede utilizar la sección como guía y ejecutar los mandatos administrativos desde una línea de mandatos. También puede copiarla, modificarla y ejecutarla en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.NORMAL.MODE.                                                                                                                                                                                                                                        |
| VOLUME.HISTORY.FILE           | Contiene una copia de la información histórica de volúmenes en el momento de la creación del plan de recuperación. El programa de utilidad DSMSERV RESTORE DB utiliza el archivo de historial de volumen para determinar qué volúmenes son necesarios para restaurar la base de datos. El archivo de historial de volumen se utilizado por el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                                                                                                                                |
| DEVICE.CONFIGURATION.FILE     | Contiene una copia de la información de configuración de dispositivos del servidor en el momento de la creación del plan de recuperación. El programa de utilidad DSMSERV RESTORE DB utiliza el archivo de configuración del dispositivo para leer los volúmenes de copia de seguridad de la base de datos. El archivo de configuración de dispositivo es utilizado por el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                                                                                                   |
| DSMSERV.OPT.FILE              | Contiene una copia del archivo de opciones del servidor. Esta sección la utiliza el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LICENSE.INFORMATION           | Contiene una copia del resultado de la auditoría de licencias más reciente y los términos del sistema de licencias del servidor.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MACHINE.GENERAL.INFORMATION   | Proporciona información para la máquina servidor, como su ubicación, que es necesaria para recrear la máquina del servidor. Esta sección se incluye en el archivo del plan si la información de máquina se ha guardado en la base de datos utilizando el mandato DEFINE MACHINE y especificando el parámetro ADSMSERVER=YES.                                                                                                                                                                                                                                |
| MACHINE.RECOVERY.INSTRUCTIONS | Proporciona las instrucciones de recuperación sobre la máquina del servidor. Esta sección se incluye en el archivo del plan si las instrucciones de recuperación de la máquina se han guardado en la base de datos.                                                                                                                                                                                                                                                                                                                                         |



| Sección                          | Información de la sección                                                                                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MACHINE.RECOVERY.CHARACTERISTICS | Proporciona las características de hardware y software para la máquina del servidor. Esta sección se incluye en el archivo del plan si las características de la máquina se han guardado en la base de datos.                                                                               |
| MACHINE.RECOVERY.MEDIA           | Proporciona información sobre los medios necesarios para recrear la máquina que contiene el servidor. Esta sección se incluye en el archivo del plan si la información de medios de recuperación se ha guardado en la base de datos y se ha asociado a la máquina que contiene el servidor. |

## Recuperación de datos de cliente y servidor utilizando DRM

Utilice la función gestor recuperación tras desastre (DRM) para recuperar el servidor de IBM Spectrum Protect y los datos de cliente cuando se produzca un siniestro.

### Antes de empezar

IBM Spectrum Protect está configurado para utilizar el protocolo SSL (capa de sockets seguros) para la autenticación de cliente/servidor. Al iniciar el servidor, se crea un archivo de certificado digital cert.kdb como parte del proceso. Este archivo incluye la clave pública del servidor, que permite al cliente cifrar datos. El archivo de certificado digital no se puede almacenar en la base de datos de servidor porque Global Security Kit (GSKit) requiere un archivo distinto en un determinado formato.

La clave de cifrado maestra está almacenada en una base de datos clave nueva gestionada por GSKit, dsmkeydb.kdb. Si el servidor ya tiene una clave de cifrado maestra, esta se migra del archivo dsmserv.pwd file a la base de datos clave, dsmkeydb.kdb. Conserve las copias de seguridad de los archivos dsmkeydb.kdb y dsmkeydb.sth. Puede configurar el mandato BACKUP DB para realizar la copia de seguridad de la clave de cifrado maestra o bien realizar usted mismo una copia de seguridad de los archivos dsmkeydb.kdb y dsmkeydb.sth de forma manual.

1. Conserve copias de seguridad de los archivos cert.kdb, cert.sth, y cert256.arm.
2. Si se han perdido o dañado tanto los archivos de certificado originales como las copias, genere nuevos archivos de certificado.

### Procedimiento

1. Obtenga el último plan de recuperación.
2. Revise los pasos de recuperación que se describen en la sección RECOVERY.INSTRUCTIONS.GENERAL del plan.
3. Separe las secciones del archivo de plan en archivos individuales para obtener instrucciones generales preliminares, scripts de recuperación de servidor de IBM Spectrum Protect e instrucciones de recuperación de cliente.
4. Recupere todos los volúmenes de recuperación necesarios (enumerados en el plan) de la caja fuerte.
5. Revise el archivo de configuración de dispositivos para asegurarse de que la configuración de hardware en el local de recuperación sea la misma que la del local original. Si hay diferencias, deben actualizarse en el archivo de configuración de dispositivos. Los siguientes cambios de configuración de ejemplo requieren actualizaciones para la información de configuración:
  - o Diferentes nombres de dispositivo.
  - o Para bibliotecas automatizadas, el requisito de colocar manualmente los volúmenes de copia de seguridad de la base de datos en la biblioteca automatizada y actualizar la información de configuración para identificar el elemento en la biblioteca. Esto permite al servidor localizar los volúmenes de copia de seguridad de la base de datos necesarios.
6. Configure hardware de sustitución para el servidor de IBM Spectrum Protect, incluyendo la instalación del sistema operativo y del release base de IBM Spectrum Protect.
7. Ejecute los scripts de recuperación del servidor de IBM Spectrum Protect desde el plan de recuperación. Las secciones RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE y RECOVERY.SCRIPT.NORMAL.MODE contienen archivos de mandatos ejecutables que se pueden utilizar para dirigir la recuperación del servidor de IBM Spectrum Protect llamando a otros archivos de mandatos que se hayan generado en el plan. El script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE recupera el servidor al punto en que los clientes pueden iniciar restauraciones directamente desde los volúmenes de agrupaciones de almacenamiento de copias.
8. Restaure las agrupaciones de almacenamiento primarias con el script RECOVERY.SCRIPT.NORMAL.MODE.
9. Inicie las operaciones de restauración de clientes por orden de mayor prioridad, según definido en su planificación de alto nivel.

### Qué hacer a continuación

El servidor IBM Spectrum Protect ya se puede utilizar para operaciones de servidor normales. Asegúrese de planificar todas las operaciones necesarias. Para obtener instrucciones, consulte Definición de planificaciones para actividades de mantenimiento del

servidor y Planificación de copia de seguridad y operaciones de archivado.

**Referencia relacionada:**

➔ PREPARE (Crear un archivo de plan de recuperación)

**Información relacionada:**

➔ Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedor de directorios

## Ejecución de obtenciones de detalles de recuperación tras desastre

---

Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

### Antes de empezar

---

Complete las siguientes tareas:

- Planifique actividades regularmente para gestionar, proteger y mantener el servidor. Para obtener más información sobre actividades planificadas, consulte Definición de planificaciones para actividades de mantenimiento del servidor. Asegúrese de planificar las siguientes tareas:
  - Realizar una copia de seguridad de la base de datos.
  - Mover medios fuera del local.
  - Realizar copia de seguridad del archivo de configuración de dispositivo, el archivo de historial de volumen y el archivo de opciones del servidor dsmserv.opt.
  - **Opcional:** Emitir el mandato PREPARE para crear el archivo del plan de recuperación tras desastre.

Consejo:

Cuando emite el mandato PREPARE, la función IBM Spectrum Protect gestor recuperación tras desastre (DRM) crea una copia del archivo del plan de recuperación tras desastre.

Puede gestionar la recuperación tras desastre fuera del local sin utilizar DRM, sin embargo, DRM ayuda a consolidar planes, scripts y otra información necesaria durante la recuperación tras desastre.

Cree múltiples copias del plan para conservarlo. Por ejemplo, mantenga copias en formato de impresión, en una unidad flash USB, en espacio de disco que se encuentra fuera del local o en un servidor remoto. El archivo del plan de recuperación tras desastre se mueve fuera del local a diario con las cintas. Para obtener más información sobre DRM, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.

- Configure los siguientes recursos en el sitio de recuperación tras desastre:
  1. Un servidor IBM Spectrum Protect de recuperación. El servidor en el sitio de recuperación de desastres debe estar en el mismo nivel que el servidor en el sitio de producción.
  2. Una biblioteca de cintas para almacenar los medios que se envían desde el sitio de producción. Para obtener más información sobre ubicaciones de recuperación fuera del local, consulte Almacenamiento de datos fuera del local.
  3. >Espacio de almacenamiento de disco para la base de datos, el registro de archivado, los registros activos y las agrupaciones de almacenamiento.
  4. Clientes para probar operaciones de restauración.

### Acerca de esta tarea

---

Pruebe el plan de recuperación tras desastre y la recuperabilidad del servidor IBM Spectrum Protect con frecuencia, en un entorno similar al entorno de producción.

### Procedimiento

---

1. Asegúrese de que las cintas estén disponibles en el local. Emita el mandato QUERY LIBVOLUME para identificar volúmenes que se dan de alta en una biblioteca automatizada.
2. Realice una copia de seguridad de la base de datos a las cintas en el local completando los pasos siguientes:
  - a. En la página Servidores del Centro de operaciones, seleccione el servidor cuya de base de datos desea hacer una copia de seguridad.
  - b. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
3. Copie los archivos siguientes en el directorio de inicio del servidor en el local de recuperación:
  - Archivo del plan de recuperación tras desastre
  - Archivo de historial de volumen
  - Archivo de configuración de dispositivo

- Opcional: archivo de opciones de servidor dsmserv.opt
- 4. Traslade la cinta a la ubicación de recuperación fuera del local.
- 5. Restaure la base de datos de servidor utilizando el programa de utilidad DSMSERV RESTORE DB en el servidor de recuperación. Para obtener más información sobre la restauración de la base de datos de servidor, consulte Restauración de la base de datos.
- 6. Emita el mandato UPDATE VOLUME y especifique el parámetro ACCESS=DESTROYED para indicar que debe restaurarse un volumen entero.
- 7. En el servidor de recuperación, restaure los volúmenes de agrupación de almacenamiento utilizando el mandato RESTORE STGPOOL.

## Qué hacer a continuación

---

Asegúrese de poder acceder a los datos de la biblioteca auditando un volumen de cinta en la agrupación de almacenamiento restaurada para verificar que los datos sean coherentes. Emita el mandato AUDIT VOLUME para auditar un volumen de cinta. Para acelerar el rendimiento, audite solo los datos restaurados.

### Tareas relacionadas:

Auditoría de inventarios de volúmenes en una biblioteca

### Referencia relacionada:

- ➔ AUDIT VOLUME (Verificar información de base de datos para un volumen de agrupación de almacenamiento)
- ➔ DSMSERV RESTORE DB (Restaurar la base de datos)
- ➔ RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento)

## Restauración de la base de datos

---

Si tiene habilitada la función gestor recuperación tras desastre (DRM) y ha seguido el procedimiento para prepararse ante un desastre, puede restaurar la base de datos después de que se produzca un desastre. Si no tiene configurado DRM, todavía podrá restaurar la base de datos, siempre que tenga los archivos de copia de seguridad necesarios.

## Antes de empezar

---

Si los directorios de la base de datos y el registro de recuperación se han perdido, vuelva a crearlos antes de ejecutar el programa de utilidad del servidor DSMSERV RESTORE DB.

## Acerca de esta tarea

---

Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Para recuperar la base de datos al instante en que se ha perdido la base de datos, recupérela a su estado actual.

Restricciones:

- Para restaurar la base de datos a la versión más reciente, debe ubicar el directorio de registro de archivado. Si no puede ubicar el directorio, puede restaurar la base de datos sólo en un momento específico.
- No puede utilizar el protocolo SSL (Secure Sockets Layer) para las operaciones de restauración de la base de datos.
- Si el nivel de release de la copia de seguridad de base de datos es diferente del nivel de release del servidor que se está restaurando, no puede restaurar la base de datos del servidor. Por ejemplo, si está utilizando un servidor de la Versión 8.1 e intenta restaurar una base de datos de la Versión 7.1, se produce un error.

## Procedimiento

---

Utilice el programa de utilidad del servidor DSMSERV RESTORE DB para restaurar la base de datos. En función de la versión de la base de datos que desee restaurar, elija uno de los siguientes métodos:

- Restaure una base de datos a su versión más reciente. Por ejemplo, utilice este mandato:

```
dsmserv restore db
```

- Restaure una base de datos a un momento específico. Por ejemplo, para restaurar la base de datos a una serie de copias de seguridad que se ha creado el 19 de abril de 2017, utilice el siguiente mandato:

```
dsmserv restore db todate=04/19/2017
```

### Referencia relacionada:

- ➔ DSMSERV RESTORE DB (Restaurar la base de datos)

## Documentación de la solución de servidor en archivos PDF

---

Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

Los siguientes archivos PDF precompilados están disponibles para soluciones de protección de datos de IBM Spectrum Protect:

- Introducción a Soluciones de protección de datos
- Guía de soluciones de disco de sitio único
- Guía de soluciones de disco multisitio
- Guía de soluciones de cintas

Para obtener más archivos PDF compilados de la documentación del servidor, consulte la lista completa.

## Servidores de IBM Spectrum Protect

Los servidores de IBM Spectrum Protect almacenan y gestionan datos de copia de seguridad, archivado y gestionados por espacio para clientes de archivado y copia de seguridad y otros componentes de IBM Spectrum Protect y IBM Spectrum Protect Snapshot.

- **Novedades**  
Obtenga información sobre las nuevas características y actualizaciones en IBM Spectrum Protect versión 8.1.
- **Instalación y actualización**  
Puede instalar o actualizar componentes individuales o múltiples en la red de la empresa. Hay documentación de soluciones disponible para ayudarle a seleccionar una solución adecuada, basándose en las necesidades de negocio y, a continuación, instalar, configurar, supervisar y operar dicha solución.
- **Configuración y gestión**  
Para completar las tareas de configuración del servidor, revise la documentación disponible.
- **Mandatos, opciones y programas de utilidad del servidor**  
Utilice mandatos para administrar y configurar el servidor, opciones para personalizar el servidor y programas de utilizar para realizar tareas especiales cuando el servidor no se está ejecutando.
- **Documentación de servidor en archivos PDF**  
Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

## Novedades

Obtenga información sobre las nuevas características y actualizaciones en IBM Spectrum Protect versión 8.1.

Consejo: Para ver vídeos sobre las nuevas características y actualizaciones, consulte la biblioteca de vídeo.

Para obtener más información sobre las nuevas características y actualizaciones, siga los enlaces de la tabla.

| Release | Nuevas características y actualizaciones                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V8.1.3  | <p>Servidor</p> <ul style="list-style-type: none"><li>• Utilizar la creación de niveles de nube para la retención de datos de larga duración</li><li>• Instalar IBM Spectrum Protect en Linux Ubuntu Server LTS</li><li>• Mejorar la seguridad del entorno de almacenamiento</li><li>• Tome medidas para proteger su sistema ante el ransomware</li></ul> <p>Centro de operaciones<br/>Actualizaciones del Centro de operaciones</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| V8.1.2  | <p>Servidor</p> <ul style="list-style-type: none"><li>• Copia de seguridad de los datos en Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube</li><li>• Cifrado de datos de cliente en una agrupación de almacenamiento de contenedores de directorio</li><li>• Copia de seguridad de un servidor de archivos NAS en una agrupación de almacenamiento de contenedores de directorio</li><li>• Instale IBM Spectrum Protect en el sistema operativo Linux on Power Systems (little endian)</li><li>• Proteja su entorno de almacenamiento con un protocolo de seguridad mejorado</li><li>• Optimización de la seguridad con la clave de cifrado maestra generada automáticamente</li><li>• Configuración de un entorno de almacenamiento utilizando la Guía de soluciones de cintas</li><li>• Planificación de actualizaciones automáticas para la copia de seguridad y restauración de clientes</li><li>• Opciones, mandatos y parámetros del servidor en desuso y sin mantenimiento</li></ul> <p>Centro de operaciones<br/>Actualizaciones del Centro de operaciones</p> |

| Release | Nuevas características y actualizaciones                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V8.1.1  | <p>Servidor</p> <ul style="list-style-type: none"> <li>• Instale IBM Spectrum Protect en el sistema operativo Linux on Power Systems (little endian)</li> <li>• Instale IBM Spectrum Protect en el sistema operativo Microsoft Windows Server 2016</li> <li>• Utilice la biblioteca de Quantum Scalar i6</li> <li>• Revise los problemas resueltos</li> </ul> <p>Centro de operaciones</p> <ul style="list-style-type: none"> <li>• Revise los problemas resueltos</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| V8.1    | <p>Servidor</p> <ul style="list-style-type: none"> <li>• Conozca IBM Spectrum Protect</li> <li>• Protección de comunicaciones mediante el protocolo TLS 1.2</li> <li>• Conversión de una agrupación de almacenamiento de cinta en una agrupación de almacenamiento de contenedores</li> <li>• Actualización de software para el gestor de la base de datos del servidor</li> <li>• El mandato REGISTER NODE ya no crea un ID de usuario de administración de forma predeterminada</li> <li>• Optimización de la autenticación de usuario en una base de datos de Active Directory</li> <li>• Aumento en la flexibilidad al proteger y reclamar volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor</li> <li>• Sistemas operativos soportados</li> <li>• Supervisión del sistema sin utilizar SNMP</li> </ul> <p>Centro de operaciones</p> <p>Actualizaciones del Centro de operaciones</p> |

- Actualizaciones del Centro de operaciones  
Hay nuevas características disponibles en IBM Spectrum Protect Operations Center Versión 8.1.3. Mediante el uso del Centro de operaciones actualizado, puede planificar actualizaciones automáticas del software del cliente de archivado y copia de seguridad de IBM Spectrum Protect y mover los datos automáticamente del almacenamiento de disco al almacenamiento en la nube para una retención de datos de larga duración.
- Actualizaciones de servidor IBM Spectrum Protect  
Hay características nuevas y otros cambios disponibles en el servidor IBM Spectrum Protect Versión 8.1.3.
- Notas del release para componentes de la versión 8.1 del servidor  
Las notas del release están disponibles para los componentes de V8.1.
- Archivos léame para componentes de la versión 8.1 del servidor  
Los archivos léame para los fixpacks de la Versión 8.1 están publicados en el sitio web de soporte de software de IBM. Pueden existir actualizaciones disponibles para los componentes del servidor, incluyendo el propio servidor, el soporte de dispositivos y el Centro de operaciones.

## Actualizaciones del Centro de operaciones

Hay nuevas características disponibles en IBM Spectrum Protect Operations Center Versión 8.1.3. Mediante el uso del Centro de operaciones actualizado, puede planificar actualizaciones automáticas del software del cliente de archivado y copia de seguridad de IBM Spectrum Protect y mover los datos automáticamente del almacenamiento de disco al almacenamiento en la nube para una retención de datos de larga duración.

Se han realizado las siguientes mejoras en Centro de operaciones:

- Puede crear planificaciones para actualizar uno o más clientes de archivado y copia de seguridad. A medida que se publican nuevos paquetes de actualizaciones, se descargan automáticamente. Cuando se ejecuta una planificación de actualizaciones, los archivos de instalación se copian en el sistema cliente y el cliente se actualiza a la versión de software especificada. También puede utilizar el Centro de operaciones para supervisar, cancelar o volver a planificar actualizaciones.
- Puede crear reglas de almacenamiento para mover automáticamente los datos de agrupaciones de almacenamiento de contenedores en directorio a agrupaciones de almacenamiento de contenedores en la nube según la antigüedad de los datos. Los distintos tipos, o *niveles*, de almacenamiento ofrecen distintas compensaciones en precio y rendimiento. Puede archivar datos más antiguos en almacenamiento de rendimiento inferior en la nube, y retener las copias de seguridad de datos recientes en un disco de alto rendimiento para acelerar las operaciones de restauración.

Para obtener más información sobre estas mejoras, consulte la ayuda de Centro de operaciones.

**Tareas relacionadas:**

Planificación de actualizaciones del cliente

## Actualizaciones de servidor IBM Spectrum Protect

---

Hay características nuevas y otros cambios disponibles en el servidor IBM Spectrum Protect Versión 8.1.3.

- Utilizar la creación de niveles de nube para la retención de datos de larga duración  
Con IBM Spectrum Protect Versión 8.1.3, puede utilizar la creación de niveles de nube para mover datos a los que se accede con poca frecuencia a una agrupación de almacenamiento de contenedores en la nube.
- Instalar IBM Spectrum Protect en Linux Ubuntu Server LTS  
Puede instalar IBM Spectrum Protect Versión 8.1.3 en el sistema operativo Ubuntu Server 16.04 LTS. Tras instalar y configurar el servidor V8.1.3 en Ubuntu Server 16.04 LTS, puede realizar una copia de seguridad de los datos en dispositivos de disco y en almacenamiento de objetos en la nube.
- Mejorar la seguridad del entorno de almacenamiento  
IBM Spectrum Protect Versión 8.1.3 proporciona mejoras de seguridad.
- Tome medidas para proteger su sistema ante el ransomware  
La documentación de IBM Spectrum Protect Versión 8.1.3 incluye directrices para ayudarle a proteger su entorno de almacenamiento frente a ataques de ransomware.

## Utilizar la creación de niveles de nube para la retención de datos de larga duración

---

Con IBM Spectrum Protect Versión 8.1.3, puede utilizar la creación de niveles de nube para mover datos a los que se accede con poca frecuencia a una agrupación de almacenamiento de contenedores en la nube.

Puede configurar IBM Spectrum Protect para almacenar datos operativos en un disco de alto rendimiento y, a continuación, mover los datos a agrupaciones de almacenamiento de contenedores en la nube a medida que envejecen. Las agrupaciones de almacenamiento de contenedores en la nube se pueden configurar para almacenamiento local o remoto en un sistema de computación en la nube Microsoft Azure o en un sistema de computación en la nube con el protocolo Simple Storage Service (S3).

Para planificar la creación de niveles de nube entre agrupaciones de almacenamiento, utilice uno de los métodos siguientes:

- En el Centro de operaciones de IBM Spectrum Protect, pulse Almacenamiento > Reglas de creación de niveles.
- Ejecute el mandato DEFINE STGRULE.

**Información relacionada:**

Definición de una regla de almacenamiento para la creación de niveles de nube

DEFINE STGRULE (Definir una regla de almacenamiento para agrupaciones de almacenamiento)

UPDATE STGRULE (Actualizar una regla de almacenamiento para agrupaciones de almacenamiento)

## Instalar IBM Spectrum Protect en Linux Ubuntu Server LTS

---

Puede instalar IBM Spectrum Protect Versión 8.1.3 en el sistema operativo Ubuntu Server 16.04 LTS. Tras instalar y configurar el servidor V8.1.3 en Ubuntu Server 16.04 LTS, puede realizar una copia de seguridad de los datos en dispositivos de disco y en almacenamiento de objetos en la nube.

Los paquetes de instalación incluyen el servidor y la licencia, las herramientas de controladores de dispositivos y el agente de almacenamiento. Se aplican las restricciones siguientes:

- No puede utilizar almacenamiento en cintas.
- No puede utilizar un gestor de recuperación tras desastre (DRM).
- No puede optimizar la transferencia de datos a servidores remotos mediante la habilitación de la tecnología Aspera® Fast Adaptive Protocol (FASP®).
- No puede configurar un entorno en clúster.
- No puede utilizar el Centro de operaciones para supervisar y gestionar el sistema.
- No puede proteger agrupaciones de almacenamiento de contenedores en directorio utilizando el mandato PROTECT STGPPOOL.

**Tareas relacionadas:**

Linux: Instalación del servidor

**Referencia relacionada:**

Linux: requisitos mínimos del servidor Linux x86\_64

**Información relacionada:**

## Mejorar la seguridad del entorno de almacenamiento

---

IBM Spectrum Protect Versión 8.1.3 proporciona mejoras de seguridad.

Los servidores, clientes y agentes de almacenamiento que utilizan IBM Spectrum Protect V8.1.3 o un software posterior, o Tivoli Storage Manager V7.1.8 o un software posterior, se configuran automáticamente para comunicarse entre sí utilizando el protocolo TLS (seguridad de la capa de transporte) 1.2. Los certificados se distribuyen automáticamente.

Restricciones:

- En V8.1.2, era necesario configurar manualmente los agentes de almacenamiento para que utilizaran SSL. A partir de V8.1.3, los agentes de almacenamiento se configuran automáticamente para utilizar SSL. Los clientes de biblioteca y servidores de gestores de bibliotecas utilizan SSL automáticamente para comunicarse con los agentes de almacenamiento que utilizan el software V7.1.8 o posterior, o el software V8.1.2 o posterior, pero debe configurar manualmente los certificados entre ellos. Un agente de almacenamiento intercambia automáticamente los certificados con su servidor de base de datos.
- Después de que un administrador se autentique correctamente utilizando el software de IBM Spectrum Protect V8.1.2 o posterior, o el software de Tivoli Storage Manager V7.1.8 o posterior, el administrador ya no se podrá autenticar en clientes ni en servidores que utilicen versiones anteriores. Esta restricción se aplica también cuando utiliza funciones como el direccionamiento de mandatos o la exportación de servidor a servidor, cuando el administrador se autentica en el servidor IBM Spectrum Protect como administrador de otro servidor.

Para obtener la información más reciente acerca de las actualizaciones de seguridad de V8.1.3, consulte la nota técnica 2004844.

**Conceptos relacionados:**

Conceptos sobre la seguridad

**Tareas relacionadas:**

Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor mediante SSL

**Referencia relacionada:**

Protección de las comunicaciones

## Tome medidas para proteger su sistema ante el ransomware

---

La documentación de IBM Spectrum Protect Versión 8.1.3 incluye directrices para ayudarle a proteger su entorno de almacenamiento frente a ataques de ransomware.

Siguiendo las directrices para configurar su entorno de almacenamiento y gestionar las políticas de retención de datos, puede reducir el riesgo de un ataque de ransomware y aumentar la posibilidad de recuperar su entorno de almacenamiento si se produce un ataque. Puede utilizar la función IBM Spectrum Protect gestor de recuperación ante siniestro (DRM) para prepararse ante ataques de ransomware y recuperarse de ellos. Puede utilizar el Centro de operaciones para supervisar atentamente su entorno de almacenamiento y detectar señales de acceso no autorizado. Revise las directrices y tome las medidas necesarias para proteger sus datos.

**Tareas relacionadas:**

Protección del entorno de almacenamiento contra ataques de ransomware

## Notas del release para componentes de la versión 8.1 del servidor

---

Las notas del release están disponibles para los componentes de V8.1.

- Notas del release para el servidor de IBM Spectrum Protect versión 8.1  
El servidor de IBM Spectrum Protect 8.1 está disponible. Incluye información de compatibilidad, instalación y otros temas de iniciación.
- Notas del release para Centro de operaciones versión 8.1  
El Centro de operaciones es una interfaz basada en web que puede utilizar para gestionar el entorno de IBM Spectrum Protect. Las notas del release le proporcionan acceso al anuncio del producto, problemas conocidos, requisitos del sistema, instrucciones de instalación y actualizaciones.
- Notas del release del soporte de dispositivos de IBM Spectrum Protect versión 8.1  
El soporte de dispositivos de IBM Spectrum Protect para V8.1 está disponible. Incluye problemas de compatibilidad, instalación y otros temas de iniciación.

## Notas del release para el servidor de IBM Spectrum Protect versión 8.1

---

El servidor de IBM Spectrum Protect 8.1 está disponible. Incluye información de compatibilidad, instalación y otros temas de iniciación.

## Contenido

---

- Descripción
- Anuncio
- Compatibilidad con versiones anteriores
- Requisitos del sistema
- Instalación y actualización de IBM Spectrum Protect
- Actualizaciones, limitaciones y problemas conocidos

## Descripción

---

IBM Spectrum Protect proporciona características de gestión de espacios, archivado y copia de seguridad automatizadas, planificadas centralmente y gestionadas mediante políticas para servidores de archivos, estaciones de trabajo, máquinas virtuales y aplicaciones.

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR resueltos, consulte la publicación APAR arreglados en el servidor de IBM Spectrum Protect, versión 8.1.

## Anuncio

---

El anuncio de la familia de productos de IBM Spectrum Protect V8.1 incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto
- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

## Compatibilidad con versiones anteriores

---

Para ver la compatibilidad con versiones anteriores, consulte la publicación Compatibilidad de cliente y servidor de IBM Spectrum Protect y consideraciones de actualización.

## Requisitos del sistema

---

Para ver la información de requisitos del sistema, consulte la publicación Sistemas operativos compatibles con IBM Spectrum Protect.

## Instalación y actualización de IBM Spectrum Protect

---

Para obtener instrucciones de instalación del servidor, consulte el procedimiento correspondiente a su sistema operativo:

IBM AIX

Instalación del servidor

Linux

Instalación del servidor

Microsoft Windows

Instalación del servidor

Para obtener instrucciones de actualización, consulte el apartado Actualización a V8.1.

## Actualizaciones, limitaciones y problemas conocidos

---

Las actualizaciones describen nueva información del producto o nuevas características del producto que pasan a estar disponibles después del lanzamiento del producto. Las actualizaciones, limitaciones y problemas conocidos están documentados en forma de



notas técnicas en la base de conocimiento de soporte de IBM® Support Portal. Pueden encontrarse soluciones o métodos alternativos para los problemas conocidos buscando en la base de conocimiento.

#### Actualizaciones

##### **El mandato REGISTER NODE ya no crea un ID de usuario de administración de forma predeterminada**

A partir de IBM Spectrum Protect V8.1, el mandato REGISTER NODE no crea automáticamente un ID de usuario de administración que coincide con el nombre de nodo. Este producto puede afectar al proceso de registro de nodos de cliente, incluidos, entre otros, los nodos del cliente de archivado y copia de seguridad de IBM Spectrum Protect. En algunos casos, puede que tenga que crear un ID de usuario de administración especificando el parámetro USERID en el mandato REGISTER NODE. Para obtener información sobre los tipos de clientes afectados, consulte la nota técnica 7048963.

Para buscar las últimas actualizaciones, consulte la publicación Actualizaciones para IBM Spectrum Protect V8.1.

#### Limitaciones y problemas conocidos

En el momento de la publicación, no existían limitaciones ni problemas conocidos.

Para buscar las limitaciones y problemas conocidos más recientes, que podrían incluir elementos adicionales, consulte Limitaciones y problemas conocidos de IBM Spectrum Protect V8.1.

## Notas del release para Centro de operaciones versión 8.1

---

El Centro de operaciones es una interfaz basada en web que puede utilizar para gestionar el entorno de IBM Spectrum Protect. Las notas del release le proporcionan acceso al anuncio del producto, problemas conocidos, requisitos del sistema, instrucciones de instalación y actualizaciones.

### Contenido

---

- Descripción
- Anuncio
- Compatibilidad con el servidor de IBM Spectrum Protect
- Requisitos del sistema
- Instalación o actualización del Centro de operaciones
- Actualizaciones, limitaciones y problemas conocidos

### Descripción

---

Puede utilizar el Centro de operaciones para realizar las acciones siguientes:

- Identificar problemas potenciales con el entorno de IBM Spectrum Protect
- Supervisar aspectos clave del entorno de almacenamiento: alertas, clientes, servidores, políticas, agrupaciones de almacenamiento y dispositivos de almacenamiento
- Registrar clientes
- Añadir servidores a supervisar
- Realizar copias de seguridad de clientes, bases de datos de servidor y agrupaciones de almacenamiento
- Iniciar la reclamación y la migración de la agrupación de almacenamiento
- Asignar alertas a para administradores y cerrar alertas
- Ver y cancelar procesos de servidor y sesiones de cliente
- Cambiar los valores del dispositivo de almacenamiento, el cliente, el servidor y la agrupación de almacenamiento
- Crear y gestionar planificaciones de cliente y ver planificaciones de administración
- Convertir agrupaciones de almacenamiento primario en agrupaciones de almacenamiento de contenedores
- Copiar datos de las agrupaciones de almacenamiento de contenedores de directorio en la cinta
- Configurar réplica
- Modificar valores de política
- Dejar fuera de servicio a los clientes y desactivar los datos
- Crear informes de correo electrónico
- Ver el uso de la capacidad frontal y de fondo para supervisar la conformidad con las licencias
- Emitir mandatos a servidores de IBM Spectrum Protect

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR arreglados, consulte la publicación APAR arreglados en el centro de operaciones de IBM Spectrum Protect versión 8.1.

### Anuncio

---

El Centro de operaciones forma parte de la familia de productos de IBM Spectrum Protect V8.1. El anuncio de estos productos incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto
- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

---

## Compatibilidad con el servidor de IBM Spectrum Protect

Para obtener información sobre la compatibilidad, consulte la publicación Compatibilidad del centro de operaciones y el servidor de IBM Spectrum Protect.

---

## Requisitos del sistema

Para obtener los requisitos del sistema, consulte la publicación Requisitos de hardware y software del centro de operaciones de IBM Spectrum Protect.

---

## Instalación o actualización del Centro de operaciones

Para obtener instrucciones de instalación, o actualizar una versión existente del Centro de operaciones, consulte Instalación y actualización del Centro de operaciones.

---

## Actualizaciones, limitaciones y problemas conocidos

Las actualizaciones describen nueva información del producto o nuevas características del producto que pasan a estar disponibles después del lanzamiento del producto. Las actualizaciones, limitaciones y problemas conocidos están documentados en forma de notas técnicas en la base de conocimiento de soporte de IBM® Support Portal. Pueden encontrarse soluciones o métodos alternativos para los problemas conocidos buscando en la base de conocimiento.

### Actualizaciones

Para obtener la lista de actualizaciones más reciente, consulte Resultados de búsqueda de actualizaciones de Centro de operaciones V8.1.

### Limitaciones y problemas conocidos

- Para obtener una lista de limitaciones y problemas conocidos, consulte Limitaciones y problemas conocidos con Centro de operaciones V8.1.
- Para buscar problemas adicionales que puedan pasar a ser problemas conocidos después del lanzamiento del producto, consulte Resultados de búsqueda de problemas conocidos con Centro de operaciones V8.1.

---

## Notas del release del soporte de dispositivos de IBM Spectrum Protect versión 8.1

El soporte de dispositivos de IBM Spectrum Protect para V8.1 está disponible. Incluye problemas de compatibilidad, instalación y otros temas de iniciación.

---

## Contenido

- Descripción
- Anuncio
- Dispositivos compatibles
- Requisitos de controladores de dispositivos
- Información de bibliotecas

- Actualizaciones, limitaciones y problemas conocidos

## Descripción

---

Este documento incluye información sobre controladores de dispositivos de IBM Spectrum Protect V8.1.

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR resueltos, consulte la publicación APAR arreglados en el controlador de dispositivo de IBM Spectrum Protect versión 8.1.

## Anuncio

---

El soporte de dispositivos de IBM Spectrum Protect para V8.1 se anuncia como parte del anuncio de los productos de la familia de IBM Spectrum Protect. El anuncio de estos productos incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto
- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

## Dispositivos admitidos

---

Para obtener información sobre los dispositivos y el hardware compatibles con sistemas IBM AIX y Microsoft Windows, consulte el apartado Dispositivos compatibles con AIX y Windows.

Para obtener información sobre el hardware y dispositivos con soporte para sistemas Linux, consulte Dispositivos compatibles con Linux.

## Requisitos de controladores de dispositivos

---

Requisitos del adaptador de bus de host

Para obtener mejores resultados, conecte las unidades de cinta y las bibliotecas de cinta al sistema con un adaptador de bus de host exclusivo. No comparta el adaptador de bus de host con otro tipo de dispositivo, como DISK o CD.

El número máximo de dispositivos soportados por los controladores de dispositivo de IBM Spectrum Protect

Para obtener información sobre el número máximo de dispositivos que los controladores de dispositivos de IBM Spectrum Protect pueden admitir en cada sistema operativo, consulte la nota técnica 1364225.

Soporte de dispositivos SAS (SCSI de conexión en serie)

Los dispositivos SAS pueden utilizarse en algunos sistemas operativos y arquitecturas. Para obtener información sobre los sistemas operativos y las arquitecturas para los dispositivos SAS, consulte la nota técnica 1396706.

Ejecución del controlador de paso a través de IBM Spectrum Protect con un ID de usuario no root en sistemas operativos Linux

Para obtener información sobre cómo permitir que un usuario no root utilice dispositivos con el controlador de paso a través de IBM Spectrum Protect en Linux, consulte la nota técnica 1321130. Utilice la opción `-g` o la opción `-a` del programa de utilidad `autoconf` del dispositivo para garantizar que los usuarios que no sean root puedan utilizar dispositivos que estén configurados con el controlador de paso a través de IBM Spectrum Protect. Utilice la opción `-g` para añadir permisos de lectura y escritura para grupos en archivos de dispositivos del controlador genérico SCSI (sg). Utilice la opción `-a` para añadir permisos de lectura y escritura para todos los usuarios en archivos de dispositivos del controlador genérico SCSI (sg).

## Información de bibliotecas

---

- Es necesario disponer de IBM Spectrum Protect Extended Edition para una biblioteca con más de cuatro unidades o más de 48 ranuras de almacenamiento.
- Es posible que las direcciones de elementos de las ranuras de almacenamiento no se correspondan directamente con los números de ranura de almacenamiento. Esto es importante porque el servidor de IBM Spectrum Protect siempre hace referencia

a las ranuras de almacenamiento por direcciones de elementos, no según los números de las ranuras de almacenamiento. Consulte la página de configuración de bibliotecas para conocer las direcciones de elementos.

- Para una biblioteca con varias unidades, se necesita una dirección de elemento de la unidad para los mandatos DEFINE y UPDATE DRIVE. No obstante, cuando la biblioteca indica los números de serie de la unidad, puede especificar ELEMENT=AUTODETECT y no es necesario conocer la dirección de elemento.
- Para el procedimiento de configuración independiente del cambiador automático y de cada unidad de la biblioteca, consulte Configuración y gestión de dispositivos de almacenamiento.

## Actualizaciones, limitaciones y problemas conocidos

### Actualizaciones

Algunos dispositivos que eran compatibles con releases anteriores de IBM Spectrum Protect ya no lo son en el servidor de IBM Spectrum Protect V8.1. Para obtener la lista más reciente de dispositivos soportados, consulte los enlaces siguientes:

- Dispositivos compatibles con AIX y Windows
- Dispositivos compatibles con Linux

Para buscar las actualizaciones, limitaciones y problemas conocidos más recientes, que podrían incluir elementos adicionales, consulte Actualizaciones, limitaciones y problemas conocidos del soporte de dispositivos de IBM Spectrum Protect V8.1.

## Archivos léame para componentes de la versión 8.1 del servidor

Los archivos léame para los fixpacks de la Versión 8.1 están publicados en el sitio web de soporte de software de IBM. Pueden existir actualizaciones disponibles para los componentes del servidor, incluyendo el propio servidor, el soporte de dispositivos y el Centro de operaciones.

Visualizar archivo léame de fixpack del servidor de IBM Spectrum Protect V8.1

## Instalación y actualización

- Implementación de una solución IBM Spectrum Protect  
Si está desplegando un nuevo entorno de servidor IBM Spectrum Protect, plantéese implementar la configuración más adecuada.
- Instalación y actualización del servidor  
El servidor de IBM Spectrum Protect proporciona servicios de copia de seguridad, archivado y gestión de espacio a clientes. Puede instalar o actualizar servidores individuales o múltiples en la red de la empresa.
- Instalación y actualización del Centro de operaciones  
Centro de operaciones es la interfaz basada en web para gestionar el entorno de almacenamiento.

## Implementación de una solución IBM Spectrum Protect

Si está desplegando un nuevo entorno de servidor IBM Spectrum Protect, plantéese implementar la configuración más adecuada.

Hay documentación de soluciones IBM Spectrum Protect disponible para ayudarle a seleccionar una solución adecuada, basándose en las necesidades de negocio y, a continuación, instalar, configurar, supervisar y operar dicha solución.

Para obtener detalles, consulte Selección de una solución IBM Spectrum Protect.










































## Disponibilidad de las características por sistema operativo

La mayoría de las características de IBM Spectrum Protect están disponibles en todos los sistemas operativos que reciben soporte para el servidor.

En la tabla siguiente, una marca de selección indica que una característica está disponible.

Tabla 1. Disponibilidad de las características de IBM Spectrum Protect por sistema operativo

| Característica | IBM® AIX | Linux x86_64 | Linux on System z | Linux on Power Systems (little endian) | Microsoft Windows |
|----------------|----------|--------------|-------------------|----------------------------------------|-------------------|
|                |          |              |                   |                                        |                   |

| Característica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | IBM® AIX                                                                            | Linux x86_64                                                                                                                                                        | Linux on System z                                                                     | Linux on Power Systems (little endian)                                                | Microsoft Windows                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Tecnología Aspera Fast Adaptive Secure Protocol (FASP): Optimización de la transferencia de datos a un servidor remoto.                                                                                                                                                                                                                                                                                                                                                                            |                                                                                     | <br>Restricción: La tecnología Aspera FASP no es compatible con Ubuntu Server LTS. |                                                                                       |                                                                                       |                                                                                       |
| Almacenamiento en la nube mediante la tecnología Amazon Simple Storage Service (Amazon S3).                                                                                                                                                                                                                                                                                                                                                                                                        |    |                                                                                    |                                                                                       |    |    |
| Almacenamiento en la nube mediante la tecnología IBM Cloud Object Storage.                                                                                                                                                                                                                                                                                                                                                                                                                         |    |                                                                                    |                                                                                       |    |    |
| Almacenamiento en la nube mediante la tecnología IBM SoftLayer (IBM Bluemix).                                                                                                                                                                                                                                                                                                                                                                                                                      |    |                                                                                    |                                                                                       |    |    |
| Almacenamiento en la nube mediante la tecnología Microsoft Azure.                                                                                                                                                                                                                                                                                                                                                                                                                                  |    |                                                                                    |                                                                                       |    |    |
| Almacenamiento en la nube mediante la tecnología OpenStack Swift.                                                                                                                                                                                                                                                                                                                                                                                                                                  |    |                                                                                    |                                                                                       |    |    |
| Deduplicación de datos:<br>Utilización de la <i>deduplicación de datos en línea</i> para eliminar datos duplicados cuando los datos se graban en una agrupación de almacenamiento del contenedor de directorio o en una agrupación de almacenamiento de contenedor en la nube. Mediante la deduplicación de datos en línea, se reduce la necesidad de realizar una reorganización fuera de línea y se puede mejorar el rendimiento del servidor y reducir el coste del hardware de almacenamiento. |  |                                                                                  |  |  |  |
| Deduplicación de datos:<br>Utilización de la <i>deduplicación de datos postproceso</i> para eliminar los datos duplicados de las agrupaciones de almacenamiento de disco de acceso secuencial. Esta opción puede aumentar los tiempos de proceso debido a que el servidor debe identificar los datos y luego eliminarlos de la agrupación de almacenamiento.                                                                                                                                       |  |                                                                                  |  |  |  |
| Gestor de recuperación ante siniestro (DRM):<br>Preparación de un plan para recuperar los datos del servidor y del cliente en caso de que se produzca un siniestro.                                                                                                                                                                                                                                                                                                                                |  |                                                                                  |  |  |  |
| Compresión de datos en línea:<br>Compresión de los datos a medida que se graban en una agrupación de almacenamiento de contenedor en la nube o de contenedor de directorio para reducir la cantidad de espacio que ocupan los datos.                                                                                                                                                                                                                                                               |  |                                                                                  |  |  |  |

| Característica                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IBM® AIX | Linux x86_64                                                                     | Linux on System z | Linux on Power Systems (little endian) | Microsoft Windows |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------|-------------------|----------------------------------------|-------------------|
| Autenticación con Lightweight Directory Access Protocol (LDAP):<br><br>Autenticación de los usuarios ante una base de datos de Active Directory en un servidor LDAP.                                                                                                                                                                                                                                                                                                   | ✓        | ✓                                                                                | ✓                 | ✓                                      | ✓                 |
| Réplica de nodos:<br>Copia incremental de los datos pertenecientes a nodos de cliente de copia de seguridad y archivado de un servidor en otro.                                                                                                                                                                                                                                                                                                                        | ✓        | ✓                                                                                | ✓                 | ✓                                      | ✓                 |
| Centro de operaciones:<br>Supervisión y gestión del entorno de almacenamiento mediante Centro de operaciones, una interfaz de usuario basada en la web.                                                                                                                                                                                                                                                                                                                | ✓        | ✓<br>Restricción:<br>El Centro de operaciones no se admite en Ubuntu Server LTS. | ✓                 | ✓                                      | ✓                 |
| Protección de agrupaciones de almacenamiento de contenedor de directorio:<br>Protección de los datos de las agrupaciones de almacenamiento de contenedor de directorio mediante el mandato PROTECT STGPOOL. Puede almacenar una copia de los datos en otra agrupación de almacenamiento de contenedor de directorio en un servidor de réplica de destino o almacenar una copia en cinta en una agrupación de almacenamiento de copia de contenedor del mismo servidor. | ✓        | ✓<br>Restricción:<br>Esta característica no tiene soporte en Ubuntu Server LTS.  | ✓                 | ✓                                      | ✓                 |
| Cifrado de agrupación de almacenamiento:<br>Cifrado de los datos de las agrupaciones de almacenamiento de contenedor de nube.                                                                                                                                                                                                                                                                                                                                          | ✓        | ✓                                                                                |                   | ✓                                      | ✓                 |
| Cifrado de agrupación de almacenamiento:<br>Cifrado de los datos de las agrupaciones de almacenamiento de contenedor de directorio.                                                                                                                                                                                                                                                                                                                                    | ✓        | ✓                                                                                | ✓                 | ✓                                      | ✓                 |
| Almacenamiento en cinta:<br>Almacenamiento de los datos en cinta, lo que proporciona una opción flexible y asequible para la conservación de datos a largo plazo.                                                                                                                                                                                                                                                                                                      | ✓        | ✓<br>Restricción:<br>No se admite almacenamiento en cintas en Ubuntu Server LTS. | ✓                 | ✓                                      | ✓                 |
| Protocolo Transport Layer Security (TLS) 1.2:<br>Protección de comunicaciones mediante el protocolo TLS 1.2                                                                                                                                                                                                                                                                                                                                                            | ✓        | ✓                                                                                | ✓                 | ✓                                      | ✓                 |

## Instalación y actualización del servidor

El servidor de IBM Spectrum Protect proporciona servicios de copia de seguridad, archivado y gestión de espacio a clientes. Puede instalar o actualizar servidores individuales o múltiples en la red de la empresa.

- Instalación del servidor en sistemas AIX
- Instalación del servidor en sistemas Linux
- Instalación del servidor en sistemas Windows
- Actualización del servidor

## AIX: Instalación del servidor

---


La instalación del servidor incluye la planificación, instalación y configuración inicial.

- AIX
- AIX: Planificación para instalar el servidor  
Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- AIX: Instalación de los componentes de servidor  
Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- AIX: Primeros pasos tras instalar IBM Spectrum Protect  
Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.
- AIX: Instalación de un fixpack de servidor de IBM Spectrum Protect  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.
- AIX: Revierta de la versión 8.1.3 a un servidor anterior  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- AIX: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- AIX: Desinstalar IBM Spectrum Protect  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## AIX: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.

- AIX: Qué debe saber primero  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- AIX: Planificación de rendimiento óptimo  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  Sistemas operativos AIX: Requisitos de sistema mínimos para sistemas AIX  
Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo AIX, en un sistema sin deduplicación de datos, revise los requisitos de hardware y software.
-  Sistemas operativos AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema  
Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.3, con algunas limitaciones.
- AIX: IBM Installation Manager  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- AIX: Hojas de trabajo para planificar detalles para el servidor  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- AIX: Planificación de la capacidad  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad,

debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.


- AIX: Prácticas más adecuadas de denominación del servidor  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- AIX: Directorios de instalación  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

## AIX: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 **Sistemas operativos AIX Restricción:** Puede instalar y ejecutar el servidor de la versión 8.1.3 en un sistema que ya tenga DB2 instalado, tanto si DB2 se ha instalado de forma independiente como si se ha instalado como parte de otra aplicación, con algunas restricciones. Para conocer más detalles, consulte el tema sobre compatibilidad con otros productos DB2.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.3 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## AIX: Planificación de rendimiento óptimo

---

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.

### Procedimiento

---


1. Revise AIX: Qué debe saber primero.
2. Revise cada una de las siguientes subsecciones.
  - AIX: Planificación del hardware del servidor y el sistema operativo  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de discos de base de datos del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de discos de registro de recuperación del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.
  - AIX: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
  - AIX: Planificación del tipo correcto de tecnología de almacenamiento  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
  - AIX: Aplicación de prácticas recomendadas para la instalación del servidor  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

## AIX: Planificación del hardware del servidor y el sistema operativo


---



Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

| Pregunta                                                                                                                                                                                                                                              | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Más información                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul> | <p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p> <p> Sistemas operativos AIX<br/>Restricción: No utilice Active Memory Expansion (AME). Al utilizar AME, el software de IBM DB2 utiliza páginas de 4 KB en lugar de páginas de 64 KB. Cada página de 4 KB debe descomprimirse al acceder a ella, y comprimirse cuando no sea necesaria. Cuando se produce la compresión o la descompresión, DB2 y el servidor esperan para acceder a la página, lo que degrada el rendimiento del servidor.</p> | <p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p> |
| <p>¿Están configurados los discos para un rendimiento óptimo?</p>                                                                                                                                                                                     | <p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>                                                                                                                                                                                                                                                                                                                |

| Pregunta                                                                                                                                                                                | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Más información                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿El servidor tiene suficiente memoria?                                                                                                                                                  | <p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p> | <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul> |
| ¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente? | <p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>                                                                                                                                                                                                                                                                                  |

| Pregunta                                                                                          | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Más información                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?   | <p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>                                                                                                                                                                                                                                                                           | <p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> |
| ¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect? | <p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. Para obtener más información sobre el sistema de archivos preferido para su sistema operativo, consulte IBM Spectrum Protect server-supported file systems.</p>                                                                                                                           | <p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>                                                                                       |
| ¿Tiene pensado configurar suficiente espacio de paginación?                                       | <p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos AIX<br/>Utilice un mínimo de 32 GB de espacio de paginación o el 50% de su RAM, el valor que sea mayor.</p> |                                                                                                                                                                                                        |

## AIX: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

| Pregunta | Tareas, características, opciones o valores | Más información |
|----------|---------------------------------------------|-----------------|
|----------|---------------------------------------------|-----------------|

| Pregunta                                                                                                                                                                                      | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Más información                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Se encuentra la base de datos en discos rápidos de baja latencia?                                                                                                                            | <p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p> | Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.                                                                                    |
| ¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento? | <p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                  |
| Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?                                           | <p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                  |
| Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?                                                  | Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB. |

| Pregunta                                                                                                                                                                                                                                                                                                                  | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Más información                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p> | <p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <code>DB2_PARALLEL_IO</code> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <code>DB2_PARALLEL_IO</code>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p> | <p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <code>DB2_PARALLEL_IO</code>, consulte Configuración recomendada para variables de registro de IBM DB2.</p> |
| <p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>                                                                                                                                                                                                                                                   | <p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>                                                                                                                                                                                                                          | <p>La profundidad de cola predeterminada suele ser demasiado baja.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## AIX: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

| Pregunta                                                                                                                                                                                      | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Más información                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos? | Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.                                                                                                                                                                                                                                                                                                                                   | La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.                                                                                                                                                                                      |
| ¿Se encuentran los registros en discos con memoria caché de escritura no volátil?                                                                                                             | La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                              |
| ¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?                                                                                           | Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.<br><br>Registro activo<br>El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.<br><br>Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.<br><br>Registro de archivos<br>El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo. | <ul style="list-style-type: none"> <li>Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>                                                |
| ¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?                                      | El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.                                                                                                                                                                                                                                                                                                                                                                                                                | Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.<br><br>Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande. |
| Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?                                                                                                          | Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro. <ul style="list-style-type: none"> <li>Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>Utilice la duplicación en el hardware del sistema de disco.</li> </ul>                                                                                                                                                       | Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.<br><br>Para obtener más información, consulte Configuración y ajuste del registro de recuperación.                                                                                                                                                            |

## AIX: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

| Pregunta                                                                                                                                                              | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Más información                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p> | <p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$                                                                                                                                                                                                                                                                                                                                                                | <p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p> |
| <p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>                                                                                                  | <p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul> | <p>Requisitos de memoria</p>                                                                                                                                                                                          |

| Pregunta                                                                                                                                                                                                                                                          | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Más información                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>                                                                                                                      | <p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p> | <p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>                                                                                            |
| <p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>                                                                                                                                                | <p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>                                                                                                 |
| <p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p> | <p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p> |
| <p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>                                                                                       | <p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>                                                                 |



| Pregunta                                                                                                                | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Más información                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <p>¿Ha asignado suficiente espacio de almacenamiento para la base de datos?</p>                                         | <p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>                                                                                                                                                                   |                                                                                                                                 |
| <p>¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?</p> | <p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol> | <p>Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.</p> |

| Pregunta                                                                                   | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Más información                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?       | <p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p> | <p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p> |
| ¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad? | <p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>                                                                                                            |
| ¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?                | <p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>                                                                                                                                                                                                                       | <p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>                                                                                                                                                                                           |

| Pregunta                                                                                                                | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Más información                                                                              |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <p>¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?</p>              | <p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>Para obtener más información, consulte la opción de cliente <code>enablededup</code>.</p> |
| <p>¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?</p> | <p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato <code>DEFINE STGPOOLDIRECTORY</code>.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                              |
| <p>¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?</p>               | <p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul> |                                                                                              |

| Pregunta                                                           | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Más información |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <p>¿Ha seleccionado el tipo apropiado de almacenamiento local?</p> | <p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul> |                 |

## AIX: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

| Pregunta | Tareas, características, opciones o valores | Más información |
|----------|---------------------------------------------|-----------------|
|----------|---------------------------------------------|-----------------|

| Pregunta                                                                                                                                                                                                                  | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Más información                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo? | <p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p> | Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.                                                                                                                                                                                                |
| ¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?                                                                                                                                        | Utilice más memoria caché para un mejor rendimiento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                             |
| En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?                          | Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario. |
| Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?                                                                                    | <p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>                                                               |
| Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?                                                      | Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.                                                                                                                       |

| Pregunta                                                                                                                                                                                                                                                                      | Tareas, características, opciones o valores                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Más información                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?</p> | <p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p> | <p>Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.</p>                                                                                                                              |
| <p>En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?</p>                                                                      | <p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>                                                                                                                                                                                                  | <p>Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.</p>                                                                                                             |
| <p>¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?</p>                                                                                                                                            | <p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul> |

## AIX: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento

Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

| <b>Tipo de tecnología de almacenamiento</b>                                                                                                                                                                              | <b>Base de datos</b>                                                                                                                                                                                                                                                                                                                                                              | <b>Registro activo</b>                                                                                                                                                                                                                                                                                                                                                                                           | <b>Registro de archivado y registro de migración tras error de archivado</b>                                                                                                                                                        | <b>Agrupaciones de almacenamiento</b>                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Unidad de estado sólido (SSD)</b>                                                                                                                                                                                     | <p>Coloque la base de datos en SSD en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>                                                                                                                 | <p>Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.</p>                                                                                                                                                                                                      | <p>Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>       | <p>Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>                                                                                                                                                                                                                                                                             |
| <p><b>Disco de alto rendimiento con las siguientes características:</b></p> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul> | <p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.</p> | <p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aísle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.</p> | <p>Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aísle estos registros de la base de datos y registro activo.</p> | <p>Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aísle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.</p> |

| Tipo de tecnología de almacenamiento                                                                                                                                                                      | Base de datos                                                                                                                                                                                                                                                    | Registro activo                                                                                                                                                                                                                                                                                 | Registro de archivado y registro de migración tras error de archivado                                                                                                                                                              | Agrupaciones de almacenamiento                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>• Disco de 10.000 rpm</li> <li>• Interfaz Fibre Channel o SAS</li> </ul> | Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones. | Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aísle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento. | Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aísle estos registros de la base de datos y registro activo. | Utilice disco de rendimiento medio o rendimiento alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aísle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones. |
| <b>SATA, almac. adjunto de red</b>                                                                                                                                                                        | No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.                                                                                                                                             | No utilice este almacenamiento para el registro activo.                                                                                                                                                                                                                                         | El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.                                                                                           | Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>• Los datos se leen con poca frecuencia.</li> </ul>                                                                                                                                                                                            |
| <b>Cinta y cinta virtual</b>                                                                                                                                                                              |                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                    | Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.                                                                                                                                                                                                                                                                                                                                                                           |

## AIX: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

| Práctica recomendada | Más información |
|----------------------|-----------------|
|----------------------|-----------------|



| Práctica recomendada                                                                                                                                                                        | Más información                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> | <p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>                                                                                                                                                                                                                                                                                                            |
| <p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>                                                                                                                   | <p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>                                                                                                                                                                                                                                                                                          |
| <p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>                                            | <p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul> |
| <p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>    | <p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>        | <p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |

| Práctica recomendada                                                                                                                                                                                                                      | Más información                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores. | <p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p> |
| Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.                                                                | <p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>○ Ajuste de la planificación para las operaciones diarias</li> <li>○ Lista de comprobación para la configuración de servidor</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Supervise las operaciones de forma constante.                                                                                                                                                                                             | <p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento. Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>                                                                                                                                                                                                                                                                                                                  |

## AIX: Requisitos de sistema mínimos para sistemas AIX

Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo AIX, en un sistema sin deduplicación de datos, revise los requisitos de hardware y software.

### Requisitos de software y de hardware de la instalación del servidor de IBM Spectrum Protect

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado AIX: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

| Tipo de hardware | Requisitos de hardware                  |
|------------------|-----------------------------------------|
| Hardware         | Un sistema POWER5 o posterior (64 bits) |


| Tipo de hardware | Requisitos de hardware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Espacio de disco | <p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección AIX: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p> |
| Memoria          | <p>Los siguientes son los requisitos mínimos de memoria del sistema para servidores con bases de datos hasta 500 GB, con ingestión diaria de no más de 200 GB al día:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |


## Requisitos de software

Tabla 2 describe los requisitos de software mínimos necesarios para un servidor en un sistema AIX.

Tabla 2. Requisitos de software

| Tipo de software | Requisitos mínimos de software |
|------------------|--------------------------------|
|------------------|--------------------------------|

| Tipo de software             | Requisitos mínimos de software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sistema operativo            | <p>AIX 6.1 ejecutándose en un entorno de kernel de 64 bits con los siguientes requisitos adicionales:</p> <ul style="list-style-type: none"> <li>• AIX 6.1 TL 7 y SP6.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 12.1.0.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 12.1.0.1. El conjunto de archivos se incluye en el paquete de fixpack de junio de 2008 de los componentes del entorno de tiempo de ejecución C++ de IBM® para AIX.</li> </ul> <p>AIX 7.1 en un entorno de kernel de 64 bits.</p> <ul style="list-style-type: none"> <li>• AIX 7.1 TL 4 y SP2.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 12.1.0.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 12.1.0.1. El conjunto de archivos se incluye en el paquete de fixpack de junio de 2008 de los componentes del entorno de tiempo de ejecución C++ de IBM para AIX.</li> </ul> <p>AIX 7.2 que se ejecuta en un entorno de kernel de 64 bits.</p> <ul style="list-style-type: none"> <li>• AIX 7.2 TL 0 y SP2.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 13.1.3.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 13.1.3.1.</li> </ul> <p>Para ver las últimas recomendaciones sobre los niveles de mantenimiento de AIX, consulte la nota técnica 21165448</p> <p>Para utilizar el recurso N_Port ID Virtualization (NPIV), asegúrese de que cumple los siguientes requisitos mínimos:</p> <ul style="list-style-type: none"> <li>• Servidor de E/S virtual 2.1.2 o posterior</li> <li>• AIX 7.1 o posterior</li> <li>• Un adaptador HBA compatible con el servidor de E/S virtual y AIX correspondiente</li> </ul> |
| Protocolo de comunicaciones  | Un método de comunicación configurado.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Proceso                      | Tiene que habilitarse la entrada/salida asíncrona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Controladores de dispositivo | <p>El controlador de dispositivo IBM Spectrum Protect es necesario para unidades y biblioteca de cintas que no son de IBM. El paquete del controlador de dispositivos IBM Spectrum Protect incluye herramientas del controlador del dispositivo y daemons de ACSLS.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Programa de utilidad gunzip  | El programa de utilidad gunzip debe estar disponible en el sistema para poder instalar o actualizar el servidor. Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Otro software                | <p>Se necesita el shell Korn (ksh).</p> <p> Sistemas operativos AIX Configure los puertos de terminación de entrada y salida (IOCP) en el sistema operativo.</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

 Sistemas operativos AIX

# AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.3, con algunas limitaciones.

Para instalar y utilizar otros productos que usen un producto DB2 en el mismo sistema que el servidor de IBM Spectrum Protect, asegúrese de que se cumplan los siguientes criterios:

Tabla 1. Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

| Criterio                    | Instrucciones                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nivel de versión            | El resto de productos que utilizan un producto DB2 tienen que utilizar la versión 9 de DB2 o una versión posterior. Los productos de DB2 incluyen soporte de encapsulamiento y segregación de productos desde la versión 9. A partir de esta versión, puede ejecutar varias copias de productos de DB2, en diferentes niveles de código, en el mismo sistema. Si desea detalles, consulte la información sobre varias copias de DB2 en Información sobre el producto DB2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ID de usuario y directorios | Asegúrese de que los ID de usuario, los ID de usuarios delimitados, la ubicación de la instalación, otros directorios y la información relacionada no se compartan en instalaciones de DB2. Las especificaciones deben ser distintas a partir de los ID y ubicaciones utilizados para la instalación y configuración del servidor de IBM Spectrum Protect. Si utilizó el asistente dsmsicfgx para configurar el servidor, estos son los valores especificados al ejecutar el asistente. Si utilizó el método de configuración manual, revise los procedimientos utilizados, si fuese necesario, para recordar los valores utilizados en el servidor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Asignación de recursos      | <p>Tenga en cuenta los recursos y las prestaciones del sistema en comparación con los requisitos del servidor de IBM Spectrum Protect y las otras aplicaciones que utilizan el producto de DB2. Para proporcionar recursos suficientes para el resto de aplicaciones DB2, es posible que deba modificar los ajustes del servidor IBM Spectrum Protect para que el servidor utilice menos recursos y memoria del sistema. De manera similar, si las cargas de trabajo de las demás aplicaciones de DB2 compiten con el servidor de IBM Spectrum Protect en cuanto a los recursos de memoria y del procesador, el rendimiento del servidor relacionado con la carga de trabajo de cliente prevista y otras operaciones podría verse afectado negativamente.</p> <p>Para segregar recursos y proporcionar más capacidades para el ajuste y la asignación del procesador, de la memoria y de otros recursos del sistema para varias aplicaciones, puede utilizar particiones lógicas (LPAR), particiones de carga de trabajo (WPAR) o el soporte de otra estación de trabajo virtual. Por ejemplo, ejecute una aplicación de DB2 en su propio sistema virtualizado.</p> |

## AIX: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager

- Oferta de IBM Spectrum Protect

#### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es `IBM Installation Manager`.

#### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.

#### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## AIX: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

| Elemento                                                                                                     | Espacio necesario | Número de directorios | Ubicación de los directorios |
|--------------------------------------------------------------------------------------------------------------|-------------------|-----------------------|------------------------------|
| La base de datos                                                                                             |                   |                       |                              |
| Registro activo                                                                                              |                   |                       |                              |
| Registro de archivos                                                                                         |                   |                       |                              |
| Opcional: duplicado de registro para el registro activo                                                      |                   |                       |                              |
| Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado) |                   |                       |                              |

| Elemento                                                                                                                                                                                                                  | Nombres e ID de usuario | Ubicación |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------|
| El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect                                                                               |                         |           |
| El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia                                                                                                           |                         |           |
| El nombre de instancia de la base de datos                                                                                                                                                                                |                         |           |
| El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor) |                         |           |
| El nombre del servidor; utilice un nombre exclusivo para cada servidor                                                                                                                                                    |                         |           |

## AIX: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- AIX: Estimación de los requisitos de espacio para la base de datos  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.
- AIX: Requisitos de espacio del registro de recuperación  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.
- AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- AIX: Supresión de archivos de retrotracción de instalación  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## AIX: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- AIX: Estimación de los requisitos de espacio de base de datos en función del número de archivos  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- AIX: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- AIX: El gestor de bases de datos y el espacio temporal  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## AIX: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.

- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.

En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:



$$500 * 3.5 = 1.7 \text{ TB}$$

## Resultados

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrece acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

| Tamaño de la base de datos | Requisito mínimo de espacio temporal |
|----------------------------|--------------------------------------|
| < 500 GB                   | 50 GB                                |
| ≥ 500 GB y < 1 TB          | 100 GB                               |
| ≥ 1 TB y < 1,5 TB          | 150 GB                               |
| ≥ 1,5 y < 2 TB             | 200 GB                               |
| ≥ 2 y < 3 TB               | 250 - 300 GB                         |
| ≥ 3 y < 4 TB               | 350 - 400 GB                         |

## AIX: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## AIX: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.
- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.
- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## AIX: Requisitos de espacio del registro de recuperación

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- AIX: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- AIX: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- AIX: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## AIX: Espacio del registro activo y archivado

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:

- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.
- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- AIX: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

$$\text{número de clientes} \times \text{archivos almacenados durante cada transacción} \\ \times \text{espacio de registro necesario para cada archivo}$$

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

| Elemento                                                                                                                                                 | Valores de ejemplo | Descripción                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento | 300                | El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche. |
| Archivos almacenados durante cada transacción                                                                                                            | 4096               | El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.                                                      |

| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Valores de ejemplo   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Espacio de registro necesario para cada archivo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 3053 bytes           | <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p> |
| Registro activo: Tamaño recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 19,5 GB <sup>1</sup> | <p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p>(300 cliente x 4096 archivos almacenados durante cada transacción x 3053 bytes para cada archivo) ÷ 1.073.741.824 bytes = 3,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p>3,5 + 16 = 19,5 GB</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Registro de archivado: Tamaño recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 58,5 GB <sup>1</sup> | <p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p>3,5 x 3 = 10,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p>10,5 + 48 = 58,5 GB</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p> |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

| Elemento | Valores de ejemplo | Descripción |
|----------|--------------------|-------------|
|----------|--------------------|-------------|

| Elemento                                                                                                                                                 | Valores de ejemplo   |                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento | 300                  | 1000                | El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Sesiones posibles para cada cliente                                                                                                                      | 3                    | 3                   | El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Archivos almacenados durante cada transacción                                                                                                            | 4096                 | 4096                | El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Espacio de registro necesario para cada archivo                                                                                                          | 3053                 | 3053                | <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>                                                                                                                                          |
| Registro activo: Tamaño recomendado                                                                                                                      | 26,5 GB <sup>1</sup> | 51 GB <sup>1</sup>  | <p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p> |
| Registro de archivado: Tamaño recomendado                                                                                                                | 79,5 GB <sup>1</sup> | 153 GB <sup>1</sup> | <p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Valores de ejemplo | Descripción |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------|
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p> |                    |             |

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

| Elemento                                                                                                                                                 | Valores de ejemplo | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento | 300                | El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Archivos almacenados durante cada transacción                                                                                                            | 4096               | El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Espacio de registro necesario para cada archivo                                                                                                          | 3453 bytes         | <p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p> |
| Registro activo: Tamaño recomendado                                                                                                                      | 20 GB <sup>1</sup> | <p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Valores de ejemplo | Descripción                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registro de archivado: Tamaño recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 60 GB <sup>1</sup> | Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:<br><br>$4 \text{ GB} \times 3 = 12 \text{ GB}$<br><br>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:<br><br>$12 + 48 = 60 \text{ GB}$ |
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p> |                    |                                                                                                                                                                                                                                                                                                                                                                                                      |

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

`300 clientes x 100.000 archivos por cada cliente x 110 bytes = 3,1 GB`

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## AIX: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.

La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

| Elemento                                                                                                                                                 | Valores de ejemplo  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento | 300                 | El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Archivos almacenados durante cada transacción                                                                                                            | 4096                | El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Espacio de registro necesario para cada archivo                                                                                                          | 3453 bytes          | <p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p> |
| Registro activo: Tamaño recomendado                                                                                                                      | 20 GB <sup>1</sup>  | <p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día                                                  | 60 GB <sup>1</sup>  | <p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana                                               | 132 GB <sup>1</sup> | <p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>                                                                                                                                                                                                                                                                                                                                        |



| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Valores de ejemplo | Descripción |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------|
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p> |                    |             |

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La

agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

| Elemento                                                                                                                                                         | Valores de ejemplo |                | Descripción                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño de un solo objeto grande del que eliminar duplicados                                                                                                      | 800 GB             | 4 TB           | La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.                                                                                                                                                 |
| Tamaño medio de extensiones                                                                                                                                      | 700 KB             | 700 KB         | El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.                                                                                                                                    |
| Extensiones para un determinado archivo                                                                                                                          | 1.198.372 bits     | 6.135.667 bits | Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.<br><br>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:<br>$(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$<br><br>Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$ |
| Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados | 1,7 GB             | 8,6 GB         | El espacio de registro activo estimado necesario para esta transacción.                                                                                                                                                                                                                                                                                                                                            |

| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Valores de ejemplo  |                       | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registro activo:<br>Tamaño total<br>recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 66 GB <sup>1</sup>  | 79,8 GB <sup>1</sup>  | <p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$ |
| Registro de<br>archivado: Tamaño<br>recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 198 GB <sup>1</sup> | 239,4 GB <sup>1</sup> | <p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$                                                                                                                                                                                                                                                                                                                                                            |
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p> |                     |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

| Elemento                                                             | Valores de ejemplo |      | Descripción                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------|--------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño de un solo<br>objeto grande del<br>que eliminar<br>duplicados | 800 GB             | 4 TB | La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado. |

| Elemento                                                                                                                                                         | Valores de ejemplo   |                       | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño medio de extensiones                                                                                                                                      | 256 KB               | 256 KB                | El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Extensiones para un determinado archivo                                                                                                                          | 3.276.800 bits       | 16.777.216 bits       | <p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.,276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados | 4,5 GB               | 23,4 GB               | El tamaño estimado del espacio de registro activo necesario para esta transacción.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Registro activo: Tamaño total recomendado                                                                                                                        | 71,6 GB <sup>1</sup> | 109,4 GB <sup>1</sup> | <p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$ |

| Elemento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Valores de ejemplo    |                       | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registro de archivado: Tamaño recomendado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 214,8 GB <sup>1</sup> | 328,2 GB <sup>1</sup> | <p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$ |
| <p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p> |                       |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## AIX: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## AIX: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## AIX: Supresión de archivos de retroacción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retroacción son tipos de archivos que puede suprimir.

## Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- AIX: Supresión de archivos de retroacción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.
- AIX: Supresión de archivos de retroacción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.


## AIX: Supresión de archivos de retroacción de instalación utilizando un asistente gráfico

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.  
 Sistemas operativos AIX En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente para iniciar IBM Installation Manager:  

```
./IBMIM
```
2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.




## AIX: Supresión de archivos de retroacción de instalación utilizando la línea de mandatos

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos AIX/eclipse/tools
 Por ejemplo:
  -  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
  -  Sistemas operativos AIX ./imcl -c
3. Especifique **P** para seleccionar Preferencias.
4. Especifique **3** para seleccionar Archivos a restaurar.
5. Especifique **D** para Suprimir los Archivos a restaurar.
6. Especifique **A** para Aplicar cambios y volver al menú Preferencias.
7. Especifique **C** para salir del Menú Preferencias.
8. Especifique **X** para Salir de Installation Manager.

## AIX: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.

### Identificador de usuario de la instancia


---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de

usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.

 Sistemas operativos AIX


## Directorio de inicio del ID de usuario de la instancia

---

El directorio de inicio puede crearse cuando se crea el ID de usuario de la instancia, utilizando la opción (-m) para crear un directorio de inicio si todavía no existe. Dependiendo de la configuración local, el directorio padre podría tener la forma:  
`/home/instance_user_ID`

Por ejemplo: `/home/tsminst1`

El directorio de inicio se utiliza principalmente como contenedor del perfil del ID de usuario y de valores de seguridad.


 Sistemas operativos AIX

## Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos tiene que ser el mismo que el identificador de usuario de la instancia en la que ejecuta la instancia del servidor.

Por ejemplo: `tsminst1`

 Sistemas operativos AIX

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede crear el directorio de la instancia como subdirectorio del directorio padre para el identificador de usuario de la instancia.  
Por ejemplo: `/home/instance_user_ID/instance_user_ID`

En el siguiente ejemplo se coloca el directorio de la instancia en el directorio padre del identificador de usuario `tsminst1`:  
`/home/tsminst1/tsminst1`

También puede crear el directorio en otra ubicación, por ejemplo: `/tsmserver/tsminst1`

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`
- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre `TSMDB1`, para todas las instancias del servidor. Este nombre no puede modificarse.

## Nombre de servidor


---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 Sistemas operativos AIX El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato `QUERY SERVER`), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.



Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.

 Sistemas operativos AIX Por ejemplo:


- PAYROLL
- SALES

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos AIX/tsminst1\_archlog

## AIX: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

`/opt/tivoli/tsm/server/bin` es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es `/opt/tivoli/tsm/db2`.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## AIX: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Con el software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones


 Sistemas operativos AIX Deje aproximadamente entre 30 y 45 minutos para instalar un servidor V 8.1.3, utilizando esta guía.

- AIX: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- AIX: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- AIX: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## AIX: Obtener el paquete de instalación

---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

 Sistemas operativos AIX

### Antes de empezar

---

Si tiene la intención de descargar los archivos, establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente:

1. Para consultar el valor de tamaño máximo de archivo, emita el mandato siguiente:


```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado siguiendo las instrucciones de la documentación de su sistema operativo.

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos AIX

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
- c. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```



- d. Extraiga el paquete emitiendo el siguiente mandato:

```
./package_name.bin
```

donde *nombre\_paquete* es el nombre del archivo descargado, por ejemplo:

 Sistemas operativos AIX

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

3.  Sistemas operativos AIX asegúrese de que el siguiente mandato esté habilitado para que los asistentes de IBM Spectrum Protect funcionen correctamente:
  -  Sistemas operativos AIX `lsuser`  
De manera predeterminada, el mandato está habilitado.
4. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - AIX: Instalación de IBM Spectrum Protect en modalidad de consola
  - AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa
5. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.


## AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación

---

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.


## Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:

-  Sistemas operativos AIX Si los siguientes archivos RPM no están instalados en el sistema, debe instalarlos. Para obtener instrucciones, consulte Instalación de archivos RPM para el asistente gráfico.
  - atk-1.12.3-2.aix5.2.ppc.rpm
  - cairo-1.8.8-1.aix5.2.ppc.rpm
  - expat-2.0.1-1.aix5.2.ppc.rpm
  - fontconfig-2.4.2-1.aix5.2.ppc.rpm
  - freetype2-2.3.9-1.aix5.2.ppc.rpm
  - gettext-0.10.40-6.aix5.1.ppc.rpm
  - glib2-2.12.4-2.aix5.2.ppc.rpm
  - gtk2-2.10.6-4.aix5.2.ppc.rpm
  - libjpeg-6b-6.aix5.1.ppc.rpm
  - libpng-1.2.32-2.aix5.2.ppc.rpm
  - libtiff-3.8.2-1.aix5.2.ppc.rpm
  - pango-1.14.5-4.aix5.2.ppc.rpm
  - pixman-0.12.0-3.aix5.2.ppc.rpm
  - xcursor-1.1.7-3.aix5.2.ppc.rpm
  - xft-2.1.6-5.aix5.1.ppc.rpm
  - xrender-0.9.1-3.aix5.2.ppc.rpm
  - zlib-1.2.3-3.aix5.1.ppc.rpm
- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:

| Opción                                                    | Descripción                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Instalación del software de un paquete descargado:</b> | <ol style="list-style-type: none"><li>Cambie al directorio donde ha descargado el paquete.</li><li>Inicie el asistente de instalación emitiendo el mandato siguiente:<br/> Sistemas operativos AIX<br/><pre>./install.sh</pre></li></ol> |

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.  
  
Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos AIX AIX: Instalación de los archivos RPM de requisito previo para el asistente gráfico  
Antes de poder utilizar el asistente gráfico de IBM Installation Manager para instalar IBM Spectrum Protect, debe asegurarse de que los archivos RPM necesarios estén instalados.

## AIX: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.


## Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:



- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:

| Opción                                                    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Instalación del software de un paquete descargado:</b> | <p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p> <pre> Sistemas operativos AIX ./install.sh -c </pre> <p>Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique  para generar las respuestas.</p> |

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos AIX/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

### Antes de empezar

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento


1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas. Si está utilizando el archivo install\_response\_sample.xml, añada la contraseña en la línea siguiente del archivo, donde *mypassword* representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación



Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo update\_response\_sample.xml.


3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor *archivo\_respuestas* representa la vía de acceso del archivo de respuestas y el nombre del archivo:

-  Sistemas operativos AIX

```
./install.sh -s -input archivo_respuestas
-acceptLicense
```

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos AIX/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

 Sistemas operativos AIX

## AIX: Instalación de paquetes de idioma del servidor

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.


### Antes de empezar

Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.

- AIX: Idiomas locales del servidor  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- AIX: Configuración de un paquete de idiomas  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.
- AIX: Actualización de un paquete de idiomas  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## AIX: Idiomas locales del servidor

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 Sistemas operativos AIX Este paquete de idioma se instala automáticamente para la siguiente opción de idioma predeterminado para los mensajes y la ayuda del servidor de IBM Spectrum Protect:

-  Sistemas operativos AIX LANGUAGE en\_US

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera. Puede utilizar los idiomas que se muestran:



 Sistemas operativos AIX

Tabla 1. Idiomas del servidor para AIX

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
Chino, simplificado (UTF-8)	ZH_CN
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (UTF-8)	ZH_TW
Chino, tradicional (euc_tw)	zh_TW
Inglés	en_US
Inglés (UTF-8)	EN_US
Francés	fr_FR

Idioma	Valor de la opción LANGUAGE
Francés (UTF-8)	FR_FR
Alemán	de_DE
Alemán (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonés, EUC	ja_JP
Japonés, PC	Ja_JP
Japonés, UTF8	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Portugués, de Brasil	pt_BR
Portugués, de Brasil (UTF-8)	PT_BR
Ruso	ru_RU
Ruso (UTF-8)	RU_RU
Español	es_ES
Español (UTF-8)	ES_ES



 **Sistemas operativos AIX** Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.

## AIX: Configuración de un paquete de idiomas

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

### Acerca de esta tarea

 **Sistemas operativos AIX** Para definir el soporte para un determinado entorno nacional, realice una de las siguientes tareas:

- Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo:
  -  **Sistemas operativos AIX** Para utilizar el entorno `it_IT`, establezca la opción LANGUAGE en `it_IT`. Consulte AIX: Idiomas locales del servidor.
-  **Sistemas operativos AIX** Si está iniciando el servidor en segundo plano, establezca el entorno variable `LC_ALL` para que coincida con el valor que se establece en el archivo de opciones del servidor. Por ejemplo, para establecer la variable de entorno en italiano, especifique el siguiente valor:

```
exportar LC_ALL=it_IT
```

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## AIX: Actualización de un paquete de idiomas

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.

Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.




## AIX: Primeros pasos tras instalar IBM Spectrum Protect

---

Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

### Acerca de esta tarea

---

1. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado AIX: Creación del ID de usuario y de directorios para la instancia del servidor.
  2. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
    - o Utilice el asistente de configuración, el método preferido. Consulte el apartado AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
    - o Configure manualmente la nueva instancia. Consulte el apartado AIX: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
      - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte AIX: Creación de una instancia del servidor.
      - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  Sistemas operativos AIX AIX: Configuración de comunicaciones de servidor y de cliente.
      - c. Emita el mandato DSMSERV FORMAT para formatear la base de datos. Consulte el apartado AIX: Formateo de la base de datos y las anotaciones.
      - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
  3. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
  4. Inicie la instancia del servidor, si todavía no se ha iniciado.
    - o  Sistemas operativos AIX Consulte el apartado AIX: Inicio de la instancia de servidor.
  5. Registre su licencia. Consulte el apartado AIX: Registro de licencias.
  6. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
  7. Supervise el servidor. Consulte el apartado AIX: Supervisión del servidor.
- AIX: Creación del ID de usuario y de directorios para la instancia del servidor  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
  - AIX: Configuración del servidor de IBM Spectrum Protect  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
  - AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
  -  Sistemas operativos AIX AIX: Inicio de la instancia de servidor  
Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario root.
  - AIX: Detención del servidor  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
  - AIX: Registro de licencias  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
  - AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
  - AIX: Ejecución de varias instancias de servidor en un solo sistema  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
  - AIX: Supervisión del servidor  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

# AIX: Creación del ID de usuario y de directorios para la instancia del servidor


Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.


## Antes de empezar

Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado AIX: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento

1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.

 Sistemas operativos AIX


 Cree un ID de usuario y un grupo que actuarán como propietarios de la instancia del servidor.

- a. Los siguientes mandatos se pueden ejecutar desde un ID de usuario administrador que vaya a definir el usuario y el grupo. Cree el ID de usuario y el grupo en el directorio de inicio del usuario.

Restricción: El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos ( \_ ). El nombre del ID de usuario y del grupo deben cumplir las siguientes reglas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Cree, por ejemplo, el ID de usuario `tsminst1` en el grupo `tsmsrvrs`. Los siguientes ejemplos muestran cómo crear este ID de usuario y grupo utilizando mandatos del sistema operativo.


 Sistemas operativos AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

Restricción: DB2 no admite la autenticación directa de usuarios del sistema operativo a través de LDAP.

- b. Cierre sesión y, a continuación, inicie sesión en su sistema. Cambie a la cuenta de usuario que acaba de crear. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

2. Cree los directorios necesarios para el servidor.

 Cree directorios vacíos para cada elemento de la tabla y asegúrese de que los directorios son propiedad del nuevo ID de usuario que acaba de crear. Monte el almacenamiento asociado en cada directorio para el registro activo, el registro de archivado y los directorios de bases de datos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El <i>directorio de instancias</i> del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir /tsminst1</code>	
Los directorios de bases de datos	<code>mkdir /tsmdb001</code> <code>mkdir /tsmdb002</code> <code>mkdir /tsmdb003</code> <code>mkdir /tsmdb004</code>	
Directorio de registro de activo	<code>mkdir /tsmlog</code>	
Directorio de registro de archivado	<code>mkdir /tsmarchlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir /tsmlogmirror</code>	



Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir /tsmarchlogfailover</code>	

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.

## AIX: Configuración del servidor de IBM Spectrum Protect

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

### Acerca de esta tarea

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:

- **AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **AIX: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.



## AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración

El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.

### Antes de empezar

Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.


### Procedimiento

1. Asegúrese de que se cumplen los siguientes requisitos:  Sistemas operativos AIX
  - El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Window. Además, debe estar ejecutando un servidor de sistema X Window en su escritorio.
  - El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. Asegúrese también de que el servicio del daemon de SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
  - Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
  - Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
  -  Sistemas operativos AIX Abra el programa `dsmicfgx` en el directorio `/opt/tivoli/tsm/server/bin`. Este asistente sólo puede ejecutarse como usuario `root`.

Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## AIX: Configuración de la instancia del servidor manualmente

Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.


- AIX: Creación de una instancia del servidor  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato db2icrt.
-  Sistemas operativos AIX: Configuración de comunicaciones de servidor y de cliente  
Se crea un archivo de opciones de servidor de ejemplo predeterminado, dsmserv.opt.smp, durante la instalación de IBM Spectrum Protect en el directorio /opt/tivoli/tsm/server/bin. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.
- AIX: Formateo de la base de datos y las anotaciones  
Utilice el programa de utilidad DSMSEV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## AIX: Creación de una instancia del servidor


Cree una instancia de IBM Spectrum Protect emitiendo el mandato db2icrt.


### Acerca de esta tarea

Puede tener una o más instancias del servidor en una estación de trabajo.


 Importante: Antes de ejecutar el mandato db2icrt, verifique los siguientes elementos:

- El directorio padre para el usuario (/home/tsminst1) existe. Si no existe ningún directorio de inicio, debe crearlo. El directorio de instancia almacena los siguientes archivos principales generados por el servidor de IBM Spectrum Protect:
  - El archivo de opciones de servidor dsmserv.opt
  - El archivo de la base de datos de la clave del servidor, cert.kdb, y los archivos .arm (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
  - El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
  - El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
  - Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
  - El usuario existe
  - Salida de rastreo (si no está cualificada al completo)
- Existe un archivo de configuración de shell (por ejemplo, .profile) en el directorio de inicio. El usuario root y el ID de usuario de instancia deben tener permiso de escritura para este archivo. Si desea más información, consulte Información sobre el producto DB2. Busque los ajustes de variable de entorno de Linux y UNIX.

 Sistemas operativos AIX

1. Inicie sesión utilizando el ID de usuario y cree una instancia de IBM Spectrum Protect. El nombre de la instancia debe coincidir con el del usuario que sea su propietario. Utilice el mandato db2icrt y entre el mandato en una línea: 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
nombre_instancia nombre_instancia
```

Por ejemplo, si el ID de usuario de esta instancia es tsminst1, utilice el siguiente mandato para crear la instancia. Escriba el mandato en una línea. 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
tsminst1 tsminst1
```

Recuerde: A partir de este momento, utilice este ID de nuevo usuario al configurar el servidor IBM Spectrum Protect. Cierre la sesión del ID de usuario root e inicie sesión con el nuevo ID de usuario de la instancia.


2. Cambie el directorio predeterminado de la base de datos para que sea la misma que el directorio de instancia del servidor. Si tiene varios servidores, inicie sesión en el ID de la instancia para cada servidor. Emita este mandato:

```
db2 update dbm cfg using dftdbpath directorio_instancia
```

Por ejemplo, si directorio\_instancia es el ID del usuario de la instancia:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Modifique la vía de acceso a biblioteca para utilizar la versión del IBM Global Security Kit (GSKit) que está instalada con el servidor. En los siguientes ejemplos, *server\_bin\_directory* es un subdirectorio del directorio de instalación del servidor. Por ejemplo, */opt/tivoli/tsm/server/bin*.

-  Sistemas operativos AIX Emita el siguiente mandato en una sola línea:

```
export LIBPATH=server_bin_directory/dbbkapi:
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```


- Debe actualizar los archivos siguientes para establecer la vía de acceso a biblioteca cuando se inicia DB2 o el servidor:

Ejemplo de shell Korn o bash:

```
directorio_inicio_usuarios_instancia/sqllib/userprofile
```

Ejemplo de C shell:

```
directorio_inicio_usuarios_instancia/sqllib/usercshrc
```


- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/userprofile* (shell Bash o Korn), en una línea:  Sistemas operativos AIX

```
export LIBPATH=server_bin_directory/
dbbkapi:/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

Recuerde: Las siguientes entradas deben estar en la vía de acceso a biblioteca:


- */usr/local/ibm/gsk8\_64/lib64*
- */opt/ibm/lib*
- */opt/ibm/lib64*
- */usr/lib64*

- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/usercshrc* (C shell), en una línea:

 Sistemas operativos AIX

```
setenv LIBPATH server_bin_directory/dbbkapi:
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

4. Cree un archivo de opciones de servidor. Consulte AIX: Configuración de comunicaciones de servidor y de cliente.

 Sistemas operativos AIX

## AIX: Configuración de comunicaciones de servidor y de cliente

Se crea un archivo de opciones de servidor de ejemplo predeterminado, *dsmserv.opt.smp*, durante la instalación de IBM Spectrum Protect en el directorio */opt/tivoli/tsm/server/bin*. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.

### Acerca de esta tarea

Asegúrese de que dispone de un directorio de instancias del servidor, como */tsminst1*, y copie el archivo de muestra a este directorio. Llame a este nuevo archivo *dsmserv.opt* y edite las opciones. Finalice esta configuración antes de inicializar la base de datos de servidor. Cada entrada de ejemplo o predeterminada del archivo de opciones de muestra es un comentario, una línea que empieza con un asterisco (\*). Las opciones no distinguen entre mayúsculas y minúsculas y se permiten uno o varios espacios en blanco entre las palabras clave y los valores.

Cuando modifique el archivo de opciones, siga estas indicaciones:




- Elimine el asterisco del principio de la línea para activar una opción.
- Puede empezar a especificar las opciones en cualquier columna.
- Escriba sólo una opción por línea. La opción debe ocupar sólo una línea.
- Si realiza varias entradas para una palabra clave, el servidor de IBM Spectrum Protect aplica la última.

Si modifica el archivo de opciones del servidor, deberá volver a arrancar el servidor para que los cambios surtan efecto.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- TCP/IP Versión 4 o Versión 6
- Memoria compartida
- capa de sockets seguros (SSL)

Consejo: Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.

-  Sistemas operativos AIXAIX: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos AIXAIX: Establecimiento de opciones de memoria compartida  
Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.
-  Sistemas operativos AIXAIX: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## AIX: Establecimiento de opciones de TCP/IP

---

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea

---

Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.


```
commmethod tcpip
tcpport 1500
tcpwindowsize 0
tcpnodelay yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPORT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.

#### Sistemas operativos AIXTCPWINDOWSIZE

 Sistemas operativos AIXEspecifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Puede especificar un entero de 0 a 2048. Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPORT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## AIX: Establecimiento de opciones de memoria compartida

---

Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.

### Acerca de esta tarea

---


El siguiente ejemplo muestra un valor de memoria compartida:


```
commmethod sharedmem
shmport 1510
```

En este ejemplo, SHMPORT especifica la dirección de puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Utilice la opción SHMPORT para especificar un puerto TCP/IP diferente. La dirección de puerto predeterminada es 1510.

COMMETHOD se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:

```
commethod tcpip
commethod sharedmem
```

 Sistemas operativos AIX El número máximo de sesiones simultáneas de memoria compartida está basado en los recursos del sistema disponibles. Cada sesión de memoria compartida utiliza una región de memoria compartida de hasta 4 MB, y cuatro colas de mensaje IPCS, dependiendo del nivel de cliente IBM Spectrum Protect.

 Sistemas operativos AIX Si el servidor y el cliente no se ejecutan con el mismo ID de usuario, el servidor debe ser un usuario root. De este modo se impide que se produzcan errores de comunicación de memoria compartida.

## AIX: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.

## AIX: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.

Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  Sistemas operativos AIX

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Inicialización de una instancia del servidor

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es /tsminst1, emita los mandatos siguientes:  Sistemas operativos AIX

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsiz=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```


Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

 **Sistemas operativos AIX** Consejo: Si DB2 no se inicia después de emitir el mandato `DSMSERV FORMAT`, puede que tenga que inhabilitar la opción de montaje `NOSUID` del sistema de archivos. Si esta opción está establecida en el sistema de archivos que contiene el directorio de propietario de instancia de DB2, o en cualquiera de los sistemas de archivos que contienen la base de datos de DB2 o registros activos, registros de archivos, registros de migración tras error o registros duplicados, la opción debe estar inhabilitada para iniciar el sistema.

Después de inhabilitar la opción `NOSUID`, vuelva a montar el sistema de archivos y después inicie DB2 emitiendo el siguiente mandato:

```
db2start
```

#### Información relacionada:

 `DSMSERV FORMAT` (Dar formato a la base de datos y a las anotaciones)


## AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos

---

Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.


### Acerca de esta tarea

---

 **Sistemas operativos AIX** Comenzando con IBM Spectrum Protect V7.1, ya no es necesario establecer la contraseña de API durante una configuración manual del servidor. Si establece la contraseña de API durante el proceso de configuración manual, los intentos para hacer una copia de seguridad de la base de datos pueden fallar.

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos `BACKUP DB` o `RESTORE DB`.

Atención: Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 **Sistemas operativos AIX** En los siguientes mandatos, sustituya los valores de ejemplo por los valores reales. Los ejemplos utilizan `tsminst1` para el ID de usuario de instancia del servidor, `/tsminst1` para el directorio de instancia del servidor, y `/home/tsminst1` como directorio de inicio de usuarios de instancia del servidor.

1. Establezca la configuración de la variable de entorno de IBM Spectrum Protect para la instancia de la base de datos:

- Inicie la sesión utilizando el ID de usuario `tsminst1`.
- Cuando el usuario `tsminst1` inicia sesión, asegúrese de que el entorno de DB2 esté debidamente inicializado. El entorno de DB2 se inicializa ejecutando el script `/home/tsminst1/sqllib/db2profile`, que normalmente se ejecuta de forma automática desde el perfil del ID de usuario. Asegúrese de que el archivo `.profile` existe en el directorio de inicio de los usuarios de instancia, por ejemplo `/home/tsminst1/.profile`. Si `.profile` no ejecuta el script `db2profile`, agregue las siguientes líneas:

```
Si [-f /home/tsminst1/sqllib/db2profile]; entonces
 . /home/tsminst1/sqllib/db2profile
fi
```

c. En el archivo directorio\_instancia/sqllib/userprofile, añada las líneas siguientes:

```
DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
DSMI_DIR=directorio_bin_servidor/dbbkapi
DSMI_LOG=directorio_instancia_servidor
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

donde:

- `directorio_instancia` es el directorio de inicio del usuario de instancia de servidor.
- `directorio_instancia_servidor` es el directorio de instancia de servidor.
- `directorio_bin_servidor` es el directorio bin de servidor. La ubicación predeterminada es `/opt/tivoli/tsm/server/bin`.

En el archivo directorio\_instancia/sqllib/usercshrc, añada las líneas siguientes:

```
setenv DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
setenv DSMI_DIR=directorio_bin_servidor/dbbkapi
setenv DSMI_LOG=directorio_instancia_servidor
```

2. Cierre la sesión y vuelva a iniciar la sesión como `tsminst1` o emita este mandato:

```
. ~/.profile
```

Consejo: Asegúrese de que especifica un espacio en blanco después del primer carácter de punto (.)

3. Cree el archivo que se denomine `tsmdbmgr.opt` en el directorio `instancia_servidor`, que se encuentra en el directorio `/tsminst1` en este ejemplo, y añada la línea siguiente:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Recuerde: El valor para `SERVERNAME` debe ser coherente en los archivos `tsmdbmgr.opt` y `dsm.sys`.

4. Como usuario `root`, agregue las siguientes líneas al archivo de configuración IBM Spectrum Protect API `dsm.sys`. De forma predeterminada, el archivo de configuración `dsm.sys` está en la ubicación predeterminada siguiente:
  - o `directorio_bin_servidor/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

donde

- o `servername` coincide con el valor de `servername` en el archivo `tsmdbmgr.opt`.
  - o `commethod` especifica la API de cliente que se utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Este valor puede ser `tcpip` o `sharedmem`. Para obtener más información sobre la memoria compartida, consulte el paso 5.
  - o `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
  - o `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmerv.opt`.
  - o `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.
  - o `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Para asegurarse de que se puede hacer copia de seguridad de la base de datos, este valor debe ser `$_TSMDBMGR_`.
5. Opcional: configura el servidor en el cual realizar la copia de seguridad mediante el uso de una memoria compartida. De esta manera, podría reducir la carga del procesador y mejorar la capacidad. Realice los siguientes pasos:
    - a. Revise el archivo `dsmerv.opt`. Si las líneas siguientes no están en el archivo, añádalas:

```
commmethod sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

- b. En el archivo de configuración `dsm.sys`, localice las siguientes líneas:

```
commmethod tcpip
tcpserveraddr localhost
tcpport número_puerto
```

Reemplace las líneas especificadas con las siguientes líneas:

```
commmethod sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

## AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor


---

Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

### Acerca de esta tarea

---

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.


 Sistemas operativos AIX Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.

Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

## Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos AIX Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancia del servidor. Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `/opt/tivoli/tsm/server/bin`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.

- a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```

4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.


### Información relacionada:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 [Sistemas operativos AIX](#)

## AIX: Inicio de la instancia de servidor


---

Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario `root`.

### Antes de empezar

---

Asegúrese de establecer los permisos de acceso y los límites de usuario correctamente.

 Sistemas operativos AIX Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).


### Acerca de esta tarea

---

Al iniciar el servidor utilizando el ID de usuario de la instancia, se simplifica el proceso de configuración y se evitan posibles problemas. Sin embargo, en algunos casos, es posible que sea necesario iniciar el servidor con el ID de usuario `root`. Por ejemplo, es posible que



desea utilizar el ID de usuario root para garantizar que el servidor pueda acceder a determinados dispositivos. Puede configurar el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia o el ID de usuario root.


 Sistemas operativos AIX Si necesita completar un mantenimiento o tareas de reconfiguración, inicie el servidor en la modalidad de mantenimiento.

## Procedimiento

---


Para iniciar el servidor, realice una de las siguientes acciones:

- Inicie el servidor haciendo uso del ID de usuario de la instancia.


 Sistemas operativos AIX Para obtener las instrucciones, consulte Inicio del servidor desde el ID del usuario de la instancia .

- Inicie el servidor utilizando el ID de usuario root.


Para obtener instrucciones sobre cómo autorizar a los ID de usuarios root a iniciar el servidor, consulte Autorización de los ID de usuario root para iniciar el servidor (V7.1.1). Para obtener instrucciones sobre cómo iniciar el servidor utilizando el ID de usuario root, consulte el apartado Inicio del servidor desde el ID de usuario root (V7.1.1).

-  Sistemas operativos AIX Inicie el servidor automáticamente.

 Sistemas operativos AIX Para obtener instrucciones, consulte AIX: Inicio automático de los servidores.

-  Sistemas operativos AIX Inicie el servidor en modalidad de mantenimiento.

Para obtener instrucciones, consulte AIX: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos AIX

## AIX: Comprobación de los derechos de acceso y límites de usuario

---

Antes de iniciar el servidor, compruebe los derechos de acceso y límites de usuario.

### Acerca de esta tarea

---

Si no verifica los límites de usuario, conocidos también como *límitesu*, podría experimentar inestabilidad del servidor o una falla del servidor al responder. También debe verificar el límite en todo el sistema para ver el número máximo de archivos abiertos. El límite de todo el sistema debe ser mayor que o equivalente al límite de usuario.

## Procedimiento

---

1. Compruebe que el ID del usuario de la instancia del servidor tenga autorizaciones para iniciar el servidor.
2. Para la instancia del servidor que piensa iniciar, asegúrese que tiene la autoridad para leer y escribir archivos en el directorio de la instancia del servidor. Compruebe que el archivo `dsmserv.opt` existe en el directorio de la instancia del servidor y de que el archivo incluye parámetros para la instancia del servidor.
3. Si el servidor está conectado a una unidad de cinta, cambiador de recursos o dispositivo de soporte extraíble y piensa iniciar el servidor mediante el uso del ID del usuario de la instancia, otorgue acceso de lectura/escritura al ID de usuario de instancias para esos dispositivos. Para establecer los permisos, realice una de las siguientes acciones:

- Si el sistema está dedicado a IBM Spectrum Protect y solo el administrador de IBM Spectrum Protect tiene acceso, haga que el archivo especial del dispositivo sea grabable para todos los usuarios. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod +w /dev/rmtX
```

- Si el sistema cuenta con varios usuarios, puede restringir el acceso si hace que el ID de usuario de la instancia de IBM Spectrum Protect sea el propietario de los archivos especiales de dispositivo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod u+w /dev/rmtX
```

- Si se están ejecutando varias instancias de usuario en el mismo sistema, cambie el nombre de grupo, por ejemplo TAPEUSERS, y añada cada ID de usuario de instancia IBM Spectrum Protect a dicho grupo. A continuación cambie la propiedad de los archivos especiales de dispositivo para que pertenezcan al grupo TAPEUSERS y haga que sean grabables para el grupo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod g+w /dev/rmtX
```

4. Compruebe los siguientes límites de usuario con base en los lineamientos de la tabla.

Tabla 1. Valores del límite (no límite) de usuario

Tipo de límite de usuario	Valor recomendado	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	Ilimitada	<code>ilimitado -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	Ilimitada	<code>ulimit -Hd</code>
Tamaño de archivo máximo	Ilimitada	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	65536	<code>ulimit -Hn</code>
La cantidad máxima de tiempo del procesador en segundos	Ilimitada	<code>ilimitado -Ht</code>

Para modificar los límites de usuario, siga las instrucciones en la documentación del sistema operativo.


Consejo: Si planea iniciar el servidor automáticamente haciendo uso de un script, puede establecer los límites de usuario en el script.

5. Asegúrese de que el límite de usuario de procesos de usuario máximos (el valor de `nproc`) se establece en el valor mínimo sugerido de 16384.

a. Para verificar el límite de usuario actual, emita el mandato `ulimit -Hu` utilizando el ID de usuario de instancia. Por ejemplo:


```
[user@Machine ~]$ ulimit -Hu
16384
```

b. Si el límite de procesos máximos del usuario no se establece en 16384, establezca el valor en 16384.

 Sistemas operativos AIX Añada la siguiente línea al archivo `/etc/security/limits`:

```
id_usuario_instancia - nproc 16384
```

donde `id_usuario_instancia` especifica el ID de usuario de instancia de servidor.

 Sistemas operativos AIX

## AIX: Inicio del servidor con el ID de usuario de la instancia

Para iniciar el servidor desde el ID de usuario de la instancia, inicie sesión con el ID de usuario de la instancia y emita el mandato correspondiente desde el directorio de la instancia del servidor.

### Antes de empezar

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para obtener instrucciones, consulte AIX: Comprobación de los derechos de acceso y límites de usuario.


### Procedimiento

1. Inicie sesión en el sistema donde instalado IBM Spectrum Protect utilizando el ID de usuario de instancia para el servidor.
2. Si no tiene un perfil de usuario que ejecuta el script de `db2profile`, emita el siguiente mandato:


```
. /home/tsminst1/sqlllib/db2profile
```

Consejo: Para obtener instrucciones sobre cómo actualizar el script de inicio de sesión de ID de usuario para ejecutar el script `db2profile` automáticamente, consulte la documentación de DB2.


3. Inicie el servidor emitiendo el siguiente mandato en una línea desde el directorio de instancia del servidor:

 Sistemas operativos AIX


```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPsize=64K
usr/bin/dmserv
```

 Sistemas operativos AIX Asegúrese de incluir un espacio después de `SHMPsize=64K`. Al iniciar el servidor con este mandato, habilitará páginas de memoria de 64 KB en el servidor. Este valor le ayuda a optimizar el rendimiento del servidor.

Consejo: El mandato se ejecuta en primer plano para que pueda configurar un ID de administrador y conectarlo con la instancia del servidor.

 Sistemas operativos AIX Por ejemplo, si el nombre de la instancia del servidor es `tsminst1` y el directorio de la instancia de servidor es `/tsminst1`, puede iniciar la instancia emitiendo los mandatos siguientes:

```
cd /tsminst1
. ~/sqllib/db2profile
LDR_CNTRL=TEXTPSIZE=64K@DATAFSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
usr/bin/dsmserv
```

 Sistemas operativos AIX

## AIX: Inicio automático de los servidores


---

Puede configurar el servidor se inicie automáticamente durante el arranque del sistema. Utilice el script `rc.dsmserv`, que se proporciona para este fin.

### Antes de empezar

---


Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente.

 Sistemas operativos AIX Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).

### Acerca de esta tarea

---

El script `rc.dsmserv` se encuentra en el directorio de instalación del servidor, por ejemplo, en el directorio `/opt/tivoli/tsm/server/bin`.

 Sistemas operativos AIX Consejo: Si ha utilizado el asistente de actualización o el asistente de configuración, debería haber elegido iniciar el servidor automáticamente al reiniciar el sistema. Si seleccionó esa opción, se agregó automáticamente una entrada para iniciar el servidor al archivo `/etc/inittab`.

### Procedimiento

---


Si no ha utilizado un asistente para configurar el servidor, añada una entrada al archivo `/etc/inittab` para cada servidor que desee que se inicie automáticamente:

1. Establezca el nivel de ejecución en el valor que corresponde a la modalidad de varios usuarios con la red habilitada. Generalmente, el nivel de ejecución que utilizar es 2, 3, o 5, en función del sistema operativo y de su configuración. Asegúrese de que el nivel de ejecución del archivo `/etc/inittab` coincida con el nivel de ejecución del sistema operativo. Para obtener más información acerca de la modalidad multiusuario y los niveles de ejecución, consulte la documentación del sistema operativo.
2. En el mandato `rc.dsmserv` en el archivo `/etc/inittab`, especifique el ID de usuario de instancia con la opción `-u` y la ubicación del directorio de instancia de servidor con la opción `-i`. Si desea iniciar más de una instancia del servidor automáticamente, agregue una entrada para cada instancia del servidor. Para verificar la sintaxis, consulte la documentación de su sistema operativo.  
Consejo: Para iniciar automáticamente una instancia de servidor con el ID de usuario raíz, use la opción `-U`.

### Ejemplo

---


Por ejemplo, si el propietario de la instancia es `tsminst1` y el directorio de la instancia del servidor es `/home/tsminst1/tsminst1`, añada la siguiente entrada a `/etc/inittab`, en una línea:

 Sistemas operativos AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```


En este ejemplo, el ID de proceso es `tsm1`, y el nivel de ejecución es 2.


Si desea ejecutar más de una instancia del servidor, añada una entrada para cada una de las instancias. Por ejemplo, si tiene los ID de propietario `tsminst1` y `tsminst2`, y los directorios de instancia `/home/tsminst1/tsminst1` y `/home/tsminst2/tsminst2`, añada las siguientes entradas a `/etc/inittab`. Cada entrada debe estar en una línea.

 Sistemas operativos AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
-i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

#### Referencia relacionada:

 [Script de inicio del servidor: rc.dsmserv](#)

 Sistemas operativos AIX

## AIX: Inicio del servidor en modalidad de mantenimiento

---

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

### Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

### Qué hacer a continuación

---

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## AIX: Detención del servidor

---


Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

### Acerca de esta tarea

---


Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:

```
halt
```

 Sistemas operativos AIX Si no se puede conectar al servidor con un cliente administrativo y desea detener el servidor, debe cancelar el proceso utilizando el mandato kill con el número del ID de proceso (pid). El pid se muestra en la inicialización.

Importante: Antes de emitir el mandato kill, asegúrese de que conoce el ID de proceso correcto del servidor IBM Spectrum Protect. El archivo `dsmserv.v6lock`, en el directorio desde el cual se está ejecutando el servidor, se puede usar para identificar el ID de proceso del proceso que desea detener. Para mostrar el archivo, especifique:

```
cat /instance_dir/dsmserv.v6lock
```

 Sistemas operativos AIX Emita el siguiente mandato para detener el servidor:

```
kill -36 dmserv_pid
```

donde *dmserv\_pid* es el número de ID del proceso.

## AIX: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

### Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

### Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

### Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

### Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

### Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

### Ejemplo

---

Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:


```
set dbrecovery dbback
```

## AIX: Ejecución de varias instancias de servidor en un solo sistema

---

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.

Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.

 Sistemas operativos AIX El conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos de AIX: Creación de una instancia del servidor para cada instancia nueva,

incluida la creación del nuevo usuario de la instancia.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.

Puede actualizar directamente de V7.1 a V8.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.3 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

#### Tareas relacionadas:

🔗 Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## AIX: Supervisión del servidor

---

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

### Procedimiento

---

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de espacio de las anotaciones activas, pero durante poco tiempo.
  - Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.
- Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tarden más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible.  
Recuerde: Si el registro de archivado y el registro de archivado de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.  
Probablemente observará el siguiente patrón:
  - a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
  - b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.

- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## AIX: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.3 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.3, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado AIX: Revertir de la versión 8.1.3 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

### Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad

de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:



```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7.  Sistemas operativos AIX Conéctese como usuario root.
8. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
9.  Sistemas operativos AIX Cambie al directorio donde situó el archivo ejecutable y complete los pasos siguientes. Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.
  - a. Cambie los permisos de archivo emitiendo el siguiente mandato:

```
chmod a+x 8.x.x.x-IBM-SPSRV-plataforma.bin
```

donde *plataforma* indica la arquitectura en la que se va a instalar IBM Spectrum Protect.

- b. Emita el siguiente mandato para extraer los archivos de instalación:

```
./8.x.x.x-IBM-SPSRV-plataforma.bin
```

10. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.

Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.

Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

#### Asistente de instalación

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

#### Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect en modalidad de consola

#### Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.

## Resultados

---



Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation



Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos AIX/var/ibm/InstallationManager/logs
-  Sistemas operativos AIXAIX: Aplicación de un fixpack a IBM Spectrum Protect V8.1.3 en un entorno de clúster para AIX  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual. Es posible aplicar un fixpack en un entorno en clúster para AIX.

## AIX: Reverta de la versión 8.1.3 a un servidor anterior

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

### Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:

- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

### Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.3 al 8.1.2 o del 8.1.3 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.


## Pasos para recuperar la versión anterior del servidor


---

### Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

### Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato:  Sistemas operativos AIX  

```
dsmserv removedb tsmdb1
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado AIX: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.3. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato:  Sistemas operativos AIX  

```
./dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.

7. Restaure la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - o Archivo de configuración de dispositivos
  - o Archivo histórico de volúmenes
  - o El archivo de opciones de servidor (generalmente dsmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.3, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de seguridad de la base de datos. Utilice el mandato RESTORE VOLUME.  
Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:  

```
audit volume nombre_volumen fix=yes
```
11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

---

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.3, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.3.

### Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.3:

- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.3. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

### Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:
  - o Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.3.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- o Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro

REUSEDELAY para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.3. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.3, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.3.

## AIX: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect


Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.

### Finalidad

Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.

Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.

Tabla 1. Mandatos de DB2

Man dato	Descripción	Ejemplo
db2i crt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia.</p> <p>Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p> <p> Sistemas operativos AIX Este programa de utilidad está en el directorio DB2DIR/instance, donde DB2DIR representa la ubicación donde se instala la versión actual del sistema de base de datos de DB2.</p>	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre>/opt/tivoli/ts m/db2/instance / db2icrt -a server -u nombre_instanc ia nombre_instanc ia</pre>
db2s et	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> <pre>db2set</pre>
CAT ALO G DAT ABA SE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	<p>Catalogue la base de datos:</p> <pre>db2 catalog database tsmdb1</pre>
CON NEC T TO DAT ABA SE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	<p>Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:</p> <pre>db2 connect to tsmdb1</pre>

Man dato	Descripción	Ejemplo
GET DAT ABA SE CON FIG URA TIO N	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Muestre la información de configuración para un alias de base de datos:  db2 get db cfg for tsbdb1  Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.  db2 get db config for tsbdb1 show detail
GET DAT ABA SE MAN AGE R CON FIG URA TIO N	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEA LTH SNA PSH OT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsbdb1
GRA NT (Aut oriza cion es de base de dato s)	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser

Man dato	Descripción	Ejemplo
RUNSTATS	<p>Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.</p> <p>Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.</p> <p>Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.</p> <p>Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.</p>	<p>Actualice las estadísticas en una única tabla.</p> <pre>db2 runstats on table SCHEMA_NAME.TA BLE_NAME with distribution and sampled detailed indexes all</pre>
SETSCHEMA	<p>Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2.</p> <p>Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.</p>	<p>Establezca el esquema para IBM Spectrum Protect:</p> <pre>db2 set schema tsmb1</pre>
STARTDATABASEMANAGER	<p>Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Inicie el gestor de base de datos:</p> <pre>db2start</pre>
STOPDATABASEMANAGER	<p>Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.</p> <p>Este mandato no es válido en un cliente.</p> <p>El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Detenga el gestor de base de datos:</p> <pre>db2 stop dbm</pre>

## AIX: Desinstalar IBM Spectrum Protect

Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.
- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

### Acerca de esta tarea

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.
- AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- AIX: Desinstalación e instalación de IBM Spectrum Protect  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- AIX: Desinstalación de IBM Installation Manager  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

## Qué hacer a continuación

---

Consulte AIX: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico


---

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento

---

1. Inicie el Installation Manager.

 Sistemas operativos AIX En el directorio en donde se encuentra instalado Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:

```
./IBMIM
```

2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.


## AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola

---

Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.

### Procedimiento


---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos AIX/eclipse/tools

Por ejemplo:

-  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools

2. Desde el directorio herramientas, emita el siguiente mandato:

-  Sistemas operativos AIX ./imcl -c

3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique N para Siguiente.
6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
7. Especifique N para Siguiente.
8. Escriba U para Desinstalar.
9. Escriba F para Finalizar.

## AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

---

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.

### Antes de empezar

---


Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.


Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  - o  Sistemas operativos AIX/eclipse/tools

Por ejemplo:

- o  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio herramientas, emita el siguiente mandato, donde `archivo_respuestas` representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

 Sistemas operativos AIX

```
./imcl -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos AIX

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## AIX: Desinstalación e instalación de IBM Spectrum Protect


---

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.

### Acerca de esta tarea


---

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos AIX Realice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```


2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:

 Sistemas operativos AIX

```
db2 attach to instance_name
db2 get dbm cfg show detail
db2 detach
```


Mantenga un registro de la ruta de base de datos para cada instancia.

3. Desinstale IBM Spectrum Protect. Consulte el apartado AIX: Desinstalar IBM Spectrum Protect.
4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten los credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estos credenciales utilizando la variable `INSTANCE_CRED`. Puede encontrar el archivo de instancias en la siguiente ubicación:


- o  Sistemas operativos AIX/etc/tivoli/tsm/instanceList.obj
5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado AIX: Instalación de los componentes de servidor.

Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- Vuelva a crear las instancias de servidor. Consulte el apartado AIX: Creación de una instancia del servidor.  
Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos AIX

```
db2 catalog database tsmdb1
db2 attach to instance_name
db2 update dbm cfg using dftdbpath instance_directory
db2 detach
```

-  Sistemas operativos AIX Compruebe que la instancia de servidor se haya creado correctamente. Emita este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```

Si figura TS MDB1 puede iniciar el servidor.

## AIX: Desinstalación de IBM Installation Manager


---

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

### Antes de empezar

---

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.


 Sistemas operativos AIX Para ver los paquetes instalados, emita el mandato siguiente desde una línea de mandatos:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

### Procedimiento

---

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos AIX

- Abra una línea de mandatos y cambie el directorio a `/var/ibm/InstallationManager/uninstall`.
- Emita el mandato siguiente:

```
./uninstall
```

Restricción: Debe haber iniciado sesión en el sistema utilizando el ID de usuario `root`.

## Linux: Instalación del servidor

---

La instalación del servidor incluye la planificación, instalación y configuración inicial.

- Linux
- Linux: Planificación para instalar el servidor  
Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- Linux: Instalación de los componentes de servidor  
Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.





- **Linux: Primeros pasos tras instalar IBM Spectrum Protect**  
Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.
- **Linux: Instalación de un fixpack de servidor de IBM Spectrum Protect**  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.
- **Linux: Revertir de la versión 8.1.3 a un servidor anterior**  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- **Linux: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect**  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- **Linux: Desinstalar IBM Spectrum Protect**  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## Linux: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiera datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.


- **Linux: Qué debe saber primero**  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- **Linux: Planificación de rendimiento óptimo**  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  **Sistemas operativos Linux**Linux: Requisitos mínimos del sistema para sistemas Linux  
Para instalar el servidor IBM Spectrum Protect en un sistema Linux, es necesario que tenga un nivel mínimo de hardware y software, incluyendo un método de comunicación y el controlador de dispositivo más actual.
-  **Sistemas operativos Linux**Linux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema  
Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.3, con algunas limitaciones.
- **Linux: IBM Installation Manager**  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- **Linux: Hojas de trabajo para planificar detalles para el servidor**  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- **Linux: Planificación de la capacidad**  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.
- **Linux: Prácticas más adecuadas de denominación del servidor**  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- **Linux: Directorios de instalación**  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

## Linux: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 **Sistemas operativos Linux**Restricción: Puede instalar y ejecutar el servidor de la versión 8.1.3 en un sistema que ya tenga DB2 instalado, tanto si DB2 se ha instalado de forma independiente como si se ha instalado como parte de otra aplicación, con algunas restricciones. Para conocer más detalles, consulte el tema sobre compatibilidad con otros productos DB2.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores

preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.3 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Linux: Planificación de rendimiento óptimo

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.

### Procedimiento

1. Revise Linux: Qué debe saber primero.
2. Revise cada una de las siguientes subsecciones.
  - Linux: Planificación del hardware del servidor y el sistema operativo  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - Linux: Planificación de discos de base de datos del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - Linux: Planificación de discos de registro de recuperación del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - Linux: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.
  - Linux: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
  - Linux: Planificación del tipo correcto de tecnología de almacenamiento  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
  - Linux: Aplicación de prácticas recomendadas para la instalación del servidor  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.





## Linux: Planificación del hardware del servidor y el sistema operativo

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---------------------------------------------	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul>	<p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p>
<p>¿Están configurados los discos para un rendimiento óptimo?</p>	<p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿El servidor tiene suficiente memoria?	<p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p>	<p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul>
¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente?	<p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>	<p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?	<p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul>
¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect?	<p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. Para obtener más información sobre el sistema de archivos preferido para su sistema operativo, consulte IBM Spectrum Protect server-supported file systems.</p>	<p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>
¿Tiene pensado configurar suficiente espacio de paginación?	<p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos Linux Utilice un mínimo de 32 GB de espacio de paginación o el 50% de su RAM, el valor que sea mayor.</p>	
 Sistemas operativos Linux ¿Tiene pensado ajustar los parámetros de kernel tras la instalación del servidor?	 Sistemas operativos Linux Tiene que ajustar los parámetros de kernel.	 Sistemas operativos Linux Consulte la información sobre cómo ajustar los parámetros de kernel: Linux: Ajuste de los parámetros de kernel para sistemas Linux

## Linux: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
¿Se encuentra la base de datos en discos rápidos de baja latencia?	<p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p>	Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.
¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento?	<p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>	
Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?	<p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>	
Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?	Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.	El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p>	<p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <i>DB2_PARALLEL_IO</i> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <i>DB2_PARALLEL_IO</i>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>	<p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>	
<p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>	<p>La profundidad de cola predeterminada suele ser demasiado baja.</p>	<p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>

## Linux: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos?	Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.	La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.
¿Se encuentran los registros en discos con memoria caché de escritura no volátil?	La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.	
¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?	<p>Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.</p> <p>Registro activo El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.</p> <p>Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.</p> <p>Registro de archivos El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo.</p>	<ul style="list-style-type: none"> <li>• Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>• Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>
¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?	El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.	<p>Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.</p> <p>Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande.</p>
Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?	<p>Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro.</p> <ul style="list-style-type: none"> <li>• Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>• Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>• Utilice la duplicación en el hardware del sistema de disco.</li> </ul>	<p>Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.</p> <p>Para obtener más información, consulte Configuración y ajuste del registro de recuperación.</p>



# Linux: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p>	<p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$	<p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>	<p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul>	<p>Requisitos de memoria</p>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>	<p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p>	<p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>	<p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>	<p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p>	<p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>	<p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p>
<p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>	<p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>	<ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha asignado suficiente espacio de almacenamiento para la base de datos?</p>	<p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>	
<p>¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?</p>	<p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol>	<p>Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?	<p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p>	<p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad?	<p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>	<ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>
¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?	<p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>	<p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?	<p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>	Para obtener más información, consulte la opción de cliente enablededup.
¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?	<p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>	
¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?	<p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul>	

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha seleccionado el tipo apropiado de almacenamiento local?	<p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul>	

## Linux: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---------------------------------------------	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo?	<p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p>	Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.
¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?	Utilice más memoria caché para un mejor rendimiento.	
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?	Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.	Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario.
Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?	<p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>	<p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>
Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?	Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.	Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.

Pregunta	Tareas, características, opciones o valores	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?	<p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p>	<p>Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.</p>
En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?	<p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>	<p>Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.</p>
¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?	<p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>	<p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul>

## Linux: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento



Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

<b>Tipo de tecnología de almacenamiento</b>	<b>Base de datos</b>	<b>Registro activo</b>	<b>Registro de archivado y registro de migración tras error de archivado</b>	<b>Agrupaciones de almacenamiento</b>
<b>Unidad de estado sólido (SSD)</b>	Coloque la base de datos en SSD en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>	Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.	Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.	Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.
<b>Disco de alto rendimiento con las siguientes características:</b> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul>	Utilice discos de alto rendimiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Utilice discos de alto rendimiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aísle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aísle estos registros de la base de datos y registro activo.	Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aísle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.

Tipo de tecnología de almacenamiento	Base de datos	Registro activo	Registro de archivado y registro de migración tras error de archivado	Agrupaciones de almacenamiento
<b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>• Disco de 10.000 rpm</li> <li>• Interfaz Fibre Channel o SAS</li> </ul>	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aísle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aísle estos registros de la base de datos y registro activo.	Utilice disco de rendimiento medio o rendimiento alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aísle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.
<b>SATA, almac. adjunto de red</b>	No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.	No utilice este almacenamiento para el registro activo.	El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.	Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>• Los datos se leen con poca frecuencia.</li> </ul>
<b>Cinta y cinta virtual</b>				Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.

## Linux: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

Práctica recomendada	Más información
----------------------	-----------------

<b>Práctica recomendada</b>	<b>Más información</b>
<p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p>	<p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>
<p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>
<p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>	<p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>
<p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>	<p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>
<p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>	<p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>

Práctica recomendada	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores.	<p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p>
Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.	<p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>◦ Ajuste de la planificación para las operaciones diarias</li> <li>◦ Lista de comprobación para la configuración de servidor</li> </ul>
Supervise las operaciones de forma constante.	<p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento.</p> <p>Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>




## Linux: Requisitos mínimos del sistema para sistemas Linux

Para instalar el servidor IBM Spectrum Protect en un sistema Linux, es necesario que tenga un nivel mínimo de hardware y software, incluyendo un método de comunicación y el controlador de dispositivo más actual.

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

El paquete de controladores de dispositivo de IBM Spectrum Protect no contiene un controlador de dispositivos para este sistema operativo porque se utiliza un controlador de dispositivo genérico SCSI. Configure el controlador de dispositivo antes de utilizar el servidor de IBM Spectrum Protect con dispositivos de cinta. El paquete de controladores de IBM Spectrum Protect contiene herramientas de controladores y daemons de ACSLS. Encontrará paquetes de controladores de IBM® en el sitio web de Fix Central.

Los requisitos, dispositivos soportados, paquetes de instalación de cliente y arreglos están disponibles en IBM Support Portal para IBM Spectrum Protect. Tras instalar IBM Spectrum Protect y antes de personalizarlo para su uso, vaya al sitio web y descargue y aplique cualquier arreglo aplicable.

-  Sistemas operativos LinuxLinux: Requisitos mínimos del servidor Linux x86\_64  
Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux x86\_64, revise los requisitos de hardware y software.
-  Sistemas operativos LinuxLinux: Requisitos mínimos del servidor Linux on System z  
Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux en System z, revise los requisitos de hardware y software.
-  Sistemas operativos LinuxLinux: Requisitos mínimos de servidor Linux on Power Systems (little endian)  
Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo Linux on Power Systems (little endian), revise los requisitos de hardware y software.

## Linux: Requisitos mínimos del servidor Linux x86\_64

Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux x86\_64, revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
servidor	Un procesador AMD64 o Intel EMT-64
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos de software mínimos necesarios para un servidor en un sistema Linux x86\_64.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	<p>El servidor IBM Spectrum Protect en Linux x86_64 requiere uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 6.7</li> <li>• Red Hat Enterprise Linux 7, incluyendo actualizaciones</li> <li>• SUSE Linux Enterprise Server 11, Service Pack 4 o posterior</li> <li>• SUSE Linux Enterprise Server 12</li> <li>• Ubuntu Server LTS, Versión 16.04 o posterior</li> </ul>

Tipo de software	Requisitos mínimos de software
Bibliotecas	<p>Bibliotecas GNU C, versión 2.3.3-98.38 o posterior, que están instaladas en el sistema IBM Spectrum Protect.</p> <p>Para Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (paquetes de 32 y 64 bit necesarios)</li> <li>• numactl.x86_64</li> </ul> <p>Para SUSE Linux Enterprise Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 en la versión 4.3 o posterior (se requieren paquetes de 32 bits y 64 bits)</li> </ul> <p>Para Ubuntu LTS Servers:</p> <ul style="list-style-type: none"> <li>• libaio1</li> </ul> <p>Para determinar si SELinux está instalado y en modalidad de imposición, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>• Examine el archivo <code>/etc/sysconfig/selinux</code>.</li> <li>• Ejecute el mandato del sistema operativo <code>sestatus</code>.</li> <li>• Examine el archivo <code>/var/log/messages</code> para ver avisos de SELinux.</li> </ul> <p>Para inhabilitar SELinux, realice una de las tareas siguientes:</p> <ul style="list-style-type: none"> <li>• Establezca la modalidad permisiva emitiendo el mandato <code>setenforce 0</code> como superusuario.</li> <li>• Modifique el archivo <code>/etc/sysconfig/selinux</code> y reinicie la máquina.</li> </ul>
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con cliente de IBM Spectrum Protect Linux x86_64)</li> </ul>
Proceso	<p>Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.</p>
Controladores de dispositivo	<p>El controlador del dispositivo de paso IBM Spectrum Protect se usa para dispositivos que no sean de IBM®. Utiliza la interfaz de paso SCSI para comunicarse con los dispositivos de cinta y las bibliotecas de cintas. El controlador de dispositivos Linux SCSI Generic (sg) es necesario para los controladores de cintas y las bibliotecas de cintas. El paquete de controladores de dispositivos de IBM Spectrum Protect incluye herramientas de controladores de dispositivos y daemons de ACSLS.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p> <p>Consejo: No se admite el almacenamiento en cintas en Ubuntu Server LTS.</p>
Otro software	<p>Se necesita el shell Korn (ksh).</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Linux: Requisitos mínimos del servidor Linux on System z

Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux en System z, revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware necesarios para IBM Spectrum Protect Linux en el sistema System z. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Servidor	Una partición lógica nativa de 64 bits de IBM® zSeries, IBM System z9, IBM System z10 o IBM zEnterprise System (z114 y z196) o invitado z/VM.
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos mínimos de software que se requieren para IBM Spectrum Protect Linux en el sistema System z.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Servidor	<p>El servidor de IBM Spectrum Protect en Linux en System z (arquitectura de s390x 64 bits) requiere uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 7.1</li> <li>• SUSE Linux Enterprise Server 12</li> </ul>

Tipo de software	Requisitos mínimos de software
Bibliotecas	<p>Una biblioteca GNU C, versión 2.4-31.43.6, está instalada en el sistema IBM Spectrum Protect. Para SUSE Linux Enterprise Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 en la versión 4.3 o posterior (se requieren paquetes de 32 bits y 64 bits)</li> <li>• libxlc-1.2.0.0.151119a.s390x o posterior</li> </ul> <p>Para Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits)</li> <li>• numactl.x86_64</li> <li>• libxlc-1.2.0.0.151119a.s390x o posterior</li> </ul>
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con el cliente de IBM Spectrum Protect Versión 8.1.3 Linux on System z)</li> </ul>
Proceso	Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.
Otro software	<p>Se necesita el shell Korn (ksh).</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Linux: Requisitos mínimos de servidor Linux on Power Systems (little endian)

Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo Linux on Power Systems (little endian), revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Servidor	Un servidor Linux on Power Systems (little endian) en un sistema IBM®, como uno listado en el sitio web de Linux on IBM Power Systems.



Tipo de hardware	Requisitos de hardware
Espacio de disco	<p>El espacio mínimo de disco siguiente:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>


## Requisitos de software

En el apartado Tabla 2 se describen los requisitos mínimos de software necesarios para su sistema.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	El sistema operativo Red Hat Enterprise Linux (RHEL) 7.3 con la arquitectura PPC64LE.
Bibliotecas	Bibliotecas GNU C, Versión 2.4-31.30 y posterior. libaio.so.1 (paquetes de 32 bits y 64 bits).
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con un cliente versión 8.1.3)</li> </ul>
Proceso	Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.
Otro software	<p>Se necesita el shell Korn (ksh).</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

Restricción: Los volúmenes lógicos RAW no están soportados.

 Sistemas operativos Linux

# Linux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.3, con algunas limitaciones.

Para instalar y utilizar otros productos que usen un producto DB2 en el mismo sistema que el servidor de IBM Spectrum Protect, asegúrese de que se cumplan los siguientes criterios:

Tabla 1. Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Criterio	Instrucciones
Nivel de versión	El resto de productos que utilizan un producto DB2 tienen que utilizar la versión 9 de DB2 o una versión posterior. Los productos de DB2 incluyen soporte de encapsulamiento y segregación de productos desde la versión 9. A partir de esta versión, puede ejecutar varias copias de productos de DB2, en diferentes niveles de código, en el mismo sistema. Si desea detalles, consulte la información sobre varias copias de DB2 en Información sobre el producto DB2.
ID de usuario y directorios	Asegúrese de que los ID de usuario, los ID de usuarios delimitados, la ubicación de la instalación, otros directorios y la información relacionada no se compartan en instalaciones de DB2. Las especificaciones deben ser distintas a partir de los ID y ubicaciones utilizados para la instalación y configuración del servidor de IBM Spectrum Protect. Si utilizó el asistente dsmitg para configurar el servidor, estos son los valores especificados al ejecutar el asistente. Si utilizó el método de configuración manual, revise los procedimientos utilizados, si fuese necesario, para recordar los valores utilizados en el servidor.
Asignación de recursos	Tenga en cuenta los recursos y las prestaciones del sistema en comparación con los requisitos del servidor de IBM Spectrum Protect y las otras aplicaciones que utilizan el producto de DB2. Para proporcionar recursos suficientes para el resto de aplicaciones DB2, es posible que deba modificar los ajustes del servidor IBM Spectrum Protect para que el servidor utilice menos recursos y memoria del sistema. De manera similar, si las cargas de trabajo de las demás aplicaciones de DB2 compiten con el servidor de IBM Spectrum Protect en cuanto a los recursos de memoria y del procesador, el rendimiento del servidor relacionado con la carga de trabajo de cliente prevista y otras operaciones podría verse afectado negativamente. Para segregación de recursos y proporcionar más capacidades para el ajuste y la asignación del procesador, de la memoria y de otros recursos del sistema para varias aplicaciones, puede utilizar particiones lógicas (LPAR), particiones de carga de trabajo (WPAR) o el soporte de otra estación de trabajo virtual. Por ejemplo, ejecute una aplicación de DB2 en su propio sistema virtualizado.

## Linux: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager

- Oferta de IBM Spectrum Protect

#### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es `IBM Installation Manager`.

#### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.

#### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## Linux: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarle a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

Elemento	Espacio necesario	Número de directorios	Ubicación de los directorios
La base de datos			
Registro activo			
Registro de archivos			
Opcional: duplicado de registro para el registro activo			
Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado)			

Elemento	Nombres e ID de usuario	Ubicación
El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect		
El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia		
El nombre de instancia de la base de datos		
El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor)		
El nombre del servidor; utilice un nombre exclusivo para cada servidor		

## Linux: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- Linux: Estimación de los requisitos de espacio para la base de datos  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.
- Linux: Requisitos de espacio del registro de recuperación  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.
- Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- Linux: Supresión de archivos de retrotracción de instalación  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Linux: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- Linux: Estimación de los requisitos de espacio de base de datos en función del número de archivos  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- Linux: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- Linux: El gestor de bases de datos y el espacio temporal  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## Linux: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.

- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.

En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:

## Resultados

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrece acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

Tamaño de la base de datos	Requisito mínimo de espacio temporal
< 500 GB	50 GB
≥ 500 GB y < 1 TB	100 GB
≥ 1 TB y < 1,5 TB	150 GB
≥ 1,5 y < 2 TB	200 GB
≥ 2 y < 3 TB	250 - 300 GB
≥ 3 y < 4 TB	350 - 400 GB

## Linux: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## Linux: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.
- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.
- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## Linux: Requisitos de espacio del registro de recuperación

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- Linux: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- Linux: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- Linux: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## Linux: Espacio del registro activo y archivado

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:



- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.
- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- Linux: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

número de clientes x archivos almacenados durante cada transacción  
x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.



Elemento	Valores de ejemplo	Descripción
Espacio de registro necesario para cada archivo	3053 bytes	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	19,5 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 3,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>3,5 + 16 = 19,5 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	58,5 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p><math>3,5 \times 3 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>10,5 + 48 = 58,5 \text{ GB}</math></p>
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

Elemento	Valores de ejemplo	Descripción
----------	--------------------	-------------

Elemento	Valores de ejemplo		Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	1000	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Sesiones posibles para cada cliente	3	3	El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.
Archivos almacenados durante cada transacción	4096	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3053	3053	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	26,5 GB <sup>1</sup>	51 GB <sup>1</sup>	<p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	79,5 GB <sup>1</sup>	153 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
Registro de archivado: Tamaño recomendado	60 GB <sup>1</sup>	Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:  $4 \text{ GB} \times 3 = 12 \text{ GB}$  Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:  $12 + 48 = 60 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

```
300 clientes x 100.000 archivos por cada cliente x 110 bytes = 3,1 GB
```

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## Linux: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.

La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día	60 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana	132 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La

agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.
Tamaño medio de extensiones	700 KB	700 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.
Extensiones para un determinado archivo	1.198.372 bits	6.135.667 bits	Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.  Se ha utilizado el siguiente cálculo para un objeto de 800 GB: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$  Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	1,7 GB	8,6 GB	El espacio de registro activo estimado necesario para esta transacción.

Elemento	Valores de ejemplo		Descripción
Registro activo: Tamaño total recomendado	66 GB <sup>1</sup>	79,8 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$
Registro de archivado: Tamaño recomendado	198 GB <sup>1</sup>	239,4 GB <sup>1</sup>	<p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.



Elemento	Valores de ejemplo		Descripción
Tamaño medio de extensiones	256 KB	256 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.
Extensiones para un determinado archivo	3.276.800 bits	16.777.216 bits	<p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.,276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	4,5 GB	23,4 GB	El tamaño estimado del espacio de registro activo necesario para esta transacción.
Registro activo: Tamaño total recomendado	71,6 GB <sup>1</sup>	109,4 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$

Elemento	Valores de ejemplo		Descripción
Registro de archivado: Tamaño recomendado	214,8 GB <sup>1</sup>	328,2 GB <sup>1</sup>	<p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

## Linux: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## Linux: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## Linux: Supresión de archivos de retroacción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retroacción son tipos de archivos que puede suprimir.

## Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.
- Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

## Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico


---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.

 Sistemas operativos Linux En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente para iniciar IBM Installation Manager:

```
./IBMIM
```

2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.

## Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos

---



Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Linux/eclipse/tools

Por ejemplo:

-  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
    -  Sistemas operativos Linux ./imcl -c
  3. Especifique **P** para seleccionar Preferencias.
  4. Especifique **3** para seleccionar Archivos a restaurar.
  5. Especifique **D** para Suprimir los Archivos a restaurar.
  6. Especifique **A** para Aplicar cambios y volver al menú Preferencias.
  7. Especifique **C** para salir del Menú Preferencias.
  8. Especifique **X** para Salir de Installation Manager.

## Linux: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.

### Identificador de usuario de la instancia


---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de

usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.

 Sistemas operativos Linux


## Directorio de inicio del ID de usuario de la instancia

---

El directorio de inicio puede crearse cuando se crea el ID de usuario de la instancia, utilizando la opción (-m) para crear un directorio de inicio si todavía no existe. Dependiendo de la configuración local, el directorio padre podría tener la forma:  
`/home/instance_user_ID`

Por ejemplo: `/home/tsminst1`

El directorio de inicio se utiliza principalmente como contenedor del perfil del ID de usuario y de valores de seguridad.


 Sistemas operativos Linux

## Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos tiene que ser el mismo que el identificador de usuario de la instancia en la que ejecuta la instancia del servidor.

Por ejemplo: `tsminst1`

 Sistemas operativos Linux

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede crear el directorio de la instancia como subdirectorio del directorio padre para el identificador de usuario de la instancia.  
Por ejemplo: `/home/instance_user_ID/instance_user_ID`

En el siguiente ejemplo se coloca el directorio de la instancia en el directorio padre del identificador de usuario `tsminst1`:  
`/home/tsminst1/tsminst1`

También puede crear el directorio en otra ubicación, por ejemplo: `/tsmserver/tsminst1`

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`
- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre `TSMDB1`, para todas las instancias del servidor. Este nombre no puede modificarse.


## Nombre de servidor

---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato `QUERY SERVER`), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.

Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.

 Sistemas operativos Linux Por ejemplo:


- PAYROLL
- SALES

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos Linux/tsminst1\_archlog

## Linux: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

`/opt/tivoli/tsm/server/bin` es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es `/opt/tivoli/tsm/db2`.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## Linux: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Con el software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones


 Sistemas operativos Linux Deje aproximadamente entre 30 y 45 minutos para instalar un servidor V 8.1.3, utilizando esta guía.

- Linux: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- Linux: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- Linux: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## Linux: Obtener el paquete de instalación

---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

 Sistemas operativos Linux

### Antes de empezar

---

Si tiene la intención de descargar los archivos, establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente:

1. Para consultar el valor de tamaño máximo de archivo, emita el mandato siguiente:


```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado siguiendo las instrucciones de la documentación de su sistema operativo.

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos Linux

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
- c. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

- d. Extraiga el paquete emitiendo el siguiente mandato:

```
./package_name.bin
```

donde *nombre\_paquete* es el nombre del archivo descargado, por ejemplo:

 Sistemas operativos Linux

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - Linux: Instalación de IBM Spectrum Protect en modalidad de consola
  - Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa
4. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación

---

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.

### Antes de empezar


---

Realice las acciones siguientes antes de iniciar la instalación:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento


Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación emitiendo el mandato siguiente:</p> <p> Sistemas operativos Linux</p> <pre>./install.sh</pre>

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.

Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.

- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## Linux: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.


## Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:


- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento


Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p> <p> Sistemas operativos Linux</p> <pre>./install.sh -c</pre> <p>Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique G para generar las respuestas.</p>

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos Linux/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.



-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa

---

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

### Antes de empezar

---

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

### Procedimiento

---

1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.


Si está utilizando el archivo install\_response\_sample.xml, añada la contraseña en la línea siguiente del archivo, donde *mypassword* representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación

Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo update\_response\_sample.xml.



3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor *archivo\_respuestas* representa la vía de acceso del archivo de respuestas y el nombre del archivo:

-  Sistemas operativos Linux

```
./install.sh -s -input archivo_respuestas
-acceptLicense
```

### Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos Linux/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

 Sistemas operativos Linux

## Linux: Instalación de paquetes de idioma del servidor

---

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

### Antes de empezar


---


Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.

- **Linux: Idiomas locales del servidor**  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- **Linux: Configuración de un paquete de idiomas**  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.
- **Linux: Actualización de un paquete de idiomas**  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## Linux: Idiomas locales del servidor

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 **Sistemas operativos Linux** Este paquete de idioma se instala automáticamente para la siguiente opción de idioma predeterminado para los mensajes y la ayuda del servidor de IBM Spectrum Protect:


-  **Sistemas operativos Linux** LANGUAGE en\_US

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera. Puede utilizar los idiomas que se muestran:

 **Sistemas operativos Linux**

Tabla 1. Idiomas del servidor para Linux

IDIOMA	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chino, tradicional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Inglés de Estados Unidos	en_US
	en_US.utf8
Francés	fr_FR
	fr_FR.utf8
Alemán	de_DE
	de_DE.utf8
Italiano	it_IT
	it_IT.utf8
Japonés	ja_JP
	ja_JP.utf8
Coreano	ko_KR
	ko_KR.utf8
Portugués, de Brasil	pt_BR
	pt_BR.utf8
Ruso	ru_RU
	ru_RU.utf8
Español	es_ES
	es_ES.utf8

 **Sistemas operativos Linux** Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.


## Linux: Configuración de un paquete de idiomas



---

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

### Acerca de esta tarea

---

 **Sistemas operativos Linux** Para definir el soporte para un determinado entorno nacional, realice una de las siguientes tareas:

- Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo:
  -  **Sistemas operativos Linux** Para utilizar el entorno `it_IT`, establezca la opción LANGUAGE en `it_IT`. Consulte Linux: Idiomas locales del servidor.
-  **Sistemas operativos Linux** Si está iniciando el servidor en segundo plano, establezca el entorno variable `LC_ALL` para que coincida con el valor que se establece en el archivo de opciones del servidor. Por ejemplo, para establecer la variable de entorno en italiano, especifique el siguiente valor:

```
exportar LC_ALL=it_IT
```

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## Linux: Actualización de un paquete de idiomas

---

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

---

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.

Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.




## Linux: Primeros pasos tras instalar IBM Spectrum Protect




---

Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

### Acerca de esta tarea

---

1.  **Sistemas operativos Linux** Actualice los valores de los parámetros del kernel.
  -  **Sistemas operativos Linux** Consulte el apartado Linux: Ajuste de parámetros del kernel en sistemas Linux.
2. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado Linux: Creación del ID de usuario y de directorios para la instancia del servidor.
3. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
  - Utilice el asistente de configuración, el método preferido. Consulte el apartado Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
  - Configure manualmente la nueva instancia. Consulte el apartado Linux: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
    - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte Linux: Creación de una instancia del servidor.
    - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  **Sistemas operativos Linux** Linux: Configuración de comunicaciones de servidor y de cliente.

- c. Emita el mandato DSMSERV FORMAT para formatear la base de datos. Consulte el apartado Linux: Formateo de la base de datos y las anotaciones.
    - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
  - 4. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
  - 5. Inicie la instancia del servidor, si todavía no se ha iniciado.
    - o  Sistemas operativos Linux Consulte el apartado Linux: Inicio de la instancia de servidor.
  - 6. Registre su licencia. Consulte el apartado Linux: Registro de licencias.
  - 7. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
  - 8. Supervise el servidor. Consulte el apartado Linux: Supervisión del servidor.
-  Sistemas operativos Linux Linux: Ajuste de parámetros del kernel en sistemas Linux  
Para que IBM Spectrum Protect y DB2 se instalen y funcionen correctamente en Linux, debe actualizar los parámetros de configuración del kernel.
  - Linux: Creación del ID de usuario y de directorios para la instancia del servidor  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
  - Linux: Configuración del servidor de IBM Spectrum Protect  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
  - Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
  -  Sistemas operativos Linux Linux: Inicio de la instancia de servidor  
Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario root.
  - Linux: Detención del servidor  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
  - Linux: Registro de licencias  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
  - Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
  - Linux: Ejecución de varias instancias de servidor en un solo sistema  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
  - Linux: Supervisión del servidor  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

 Sistemas operativos Linux

## Linux: Ajuste de parámetros del kernel en sistemas Linux



---

Para que IBM Spectrum Protect y DB2 se instalen y funcionen correctamente en Linux, debe actualizar los parámetros de configuración del kernel.

### Acerca de esta tarea

---

Si no actualiza estos parámetros, la instalación de DB2 y IBM Spectrum Protect puede fallar. Aunque la instalación se realice correctamente, pueden producirse problemas operativos si no establecer valores para los parámetros.

-  Sistemas operativos Linux Linux: Actualización de parámetros del kernel en Linux  
DB2 aumenta automáticamente los valores de parámetros del kernel de comunicación entre procesos (IPC) a los valores recomendados.
-  Sistemas operativos Linux Linux: Valores recomendados para parámetros del kernel en Linux  
Asegúrese de que los valores para los parámetros del kernel sean suficientes para evitar problemas operativos al ejecutar el servidor de IBM Spectrum Protect.

## Linux: Actualización de parámetros del kernel en Linux

DB2 aumenta automáticamente los valores de parámetros del kernel de comunicación entre procesos (IPC) a los valores recomendados.

### Acerca de esta tarea

Para actualizar parámetros del kernel en servidores Linux, siga estos pasos

### Procedimiento

1. Emita el mandato `ipcs -l` para ver una lista de valores de parámetros.
2. Analice los resultados para determinar si su sistema requiere algún cambio: Si se necesitan cambios, puede definir el parámetro en el archivo `/etc/sysctl.conf`. El valor del parámetro se aplica cuando se inicia el sistema.

### Qué hacer a continuación

Para Red Hat Enterprise Linux 6 (RHEL6), debe definir el parámetro `kernel.shmmax` en el archivo `/etc/sysctl.conf` antes de iniciar automáticamente el servidor de IBM Spectrum Protect al arrancar el sistema.

Si desea detalles sobre la base de datos DB2 para Linux, consulte Información sobre el producto DB2.

## Linux: Valores recomendados para parámetros del kernel en Linux

Asegúrese de que los valores para los parámetros del kernel sean suficientes para evitar problemas operativos al ejecutar el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

La tabla siguiente contiene los valores de parámetro de kernel recomendados para ejecutar IBM Spectrum Protect y DB2.

Parámetro	Descripción	Valor recomendado
<code>kernel.randomize_va_space</code>	El parámetro <code>kernel.randomize_va_space</code> configura el uso del kernel de ASLR de memoria. Si establece el valor en 0, <code>kernel.randomize_va_space=0</code> , se inhabilita ASLR. Los servidores de datos de DB2 se basan en direcciones finas para ciertos objetos de memoria compartida y ASLR puede ocasionar errores para ciertas actividades. Para obtener más información sobre Linux ASLR y DB2, consulte la nota técnica en: <a href="http://www.ibm.com/support/docview.wss?uid=swg21365583">http://www.ibm.com/support/docview.wss?uid=swg21365583</a> .	0
<code>vm.swappiness</code>	El parámetro <code>vm.swappiness</code> define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información sobre el producto DB2.	0
<code>vm.overcommit_memory</code>	El parámetro <code>vm.overcommit_memory</code> afecta a la cantidad de memoria virtual que el kernel permite asignar. Para obtener más información sobre los parámetros del kernel, consulte Información sobre el producto DB2.	0

## Linux: Creación del ID de usuario y de directorios para la instancia del servidor

Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.


## Antes de empezar

Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado Linux: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento

1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.

### Sistemas operativos Linux

 Cree un ID de usuario y un grupo que actuarán como propietarios de la instancia del servidor.

- a. Los siguientes mandatos se pueden ejecutar desde un ID de usuario administrador que vaya a definir el usuario y el grupo. Cree el ID de usuario y el grupo en el directorio de inicio del usuario.

Restricción: El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos ( \_ ). El nombre del ID de usuario y del grupo deben cumplir las siguientes reglas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Cree, por ejemplo, el ID de usuario `tsminst1` en el grupo `tsmsrvrs`. Los siguientes ejemplos muestran cómo crear este ID de usuario y grupo utilizando mandatos del sistema operativo.


### Sistemas operativos Linux

```
groupadd tsmsrvrs -g 1111
useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
passwd tsminst1
```

Restricción: DB2 no admite la autenticación directa de usuarios del sistema operativo a través de LDAP.

- b. Cierre sesión y, a continuación, inicie sesión en su sistema. Cambie a la cuenta de usuario que acaba de crear. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

2. Cree los directorios necesarios para el servidor.

 Cree directorios vacíos para cada elemento de la tabla y asegúrese de que los directorios son propiedad del nuevo ID de usuario que acaba de crear. Monte el almacenamiento asociado en cada directorio para el registro activo, el registro de archivado y los directorios de bases de datos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El <i>directorio de instancias</i> del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir /tsminst1</code>	
Los directorios de bases de datos	<code>mkdir /tsmdb001</code> <code>mkdir /tsmdb002</code> <code>mkdir /tsmdb003</code> <code>mkdir /tsmdb004</code>	
Directorio de registro de activo	<code>mkdir /tsmlog</code>	
Directorio de registro de archivado	<code>mkdir /tsmarchlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir /tsmlogmirror</code>	
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir /tsmarchlogfailover</code>	

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.

## Linux: Configuración del servidor de IBM Spectrum Protect

---

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

### Acerca de esta tarea

---

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:

- **Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **Linux: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

## Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración

---

El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.



### Antes de empezar

---

Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.

### Procedimiento

---

1. Asegúrese de que se cumplen los siguientes requisitos:  Sistemas operativos Linux
  - El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Window. Además, debe estar ejecutando un servidor de sistema X Window en su escritorio.
  - El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. Asegúrese también de que el servicio del daemon de SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
  - Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
  - Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
  -  Sistemas operativos Linux Abra el programa `dsmicfgx` en el directorio `/opt/tivoli/tsm/server/bin`. Este asistente sólo puede ejecutarse como usuario `root`.


Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Linux: Configuración de la instancia del servidor manualmente

---

Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

- **Linux: Creación de una instancia del servidor**  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.


-  Sistemas operativos Linux: Configuración de comunicaciones de servidor y de cliente  
Se crea un archivo de opciones de servidor de ejemplo predeterminado, `dsmserv.opt.smp`, durante la instalación de IBM Spectrum Protect en el directorio `/opt/tivoli/tsm/server/bin`. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.
- Linux: Formateo de la base de datos y las anotaciones  
Utilice el programa de utilidad `DSMSERV FORMAT` para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## Linux: Creación de una instancia del servidor

Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.

### Acerca de esta tarea


Puede tener una o más instancias del servidor en una estación de trabajo.

 Sistemas operativos Linux: Importante: Antes de ejecutar el mandato `db2icrt`, verifique los siguientes elementos:


- El directorio padre para el usuario (`/home/tsminst1`) existe. Si no existe ningún directorio de inicio, debe crearlo. El directorio de instancia almacena los siguientes archivos principales generados por el servidor de IBM Spectrum Protect:
  - El archivo de opciones de servidor `dsmserv.opt`
  - El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
  - El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
  - El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
  - Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
  - El usuario existe
  - Salida de rastreo (si no está cualificada al completo)
- Existe un archivo de configuración de shell (por ejemplo, `.profile`) en el directorio de inicio. El usuario `root` y el ID de usuario de instancia deben tener permiso de escritura para este archivo. Si desea más información, consulte Información sobre el producto DB2. Busque los ajustes de variable de entorno de Linux y UNIX.

 Sistemas operativos Linux

1. Inicie sesión utilizando el ID de usuario y cree una instancia de IBM Spectrum Protect. El nombre de la instancia debe coincidir con el del usuario que sea su propietario. Utilice el mandato `db2icrt` y entre el mandato en una línea:

 Sistemas operativos Linux

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
nombre_instancia nombre_instancia
```

Por ejemplo, si el ID de usuario de esta instancia es `tsminst1`, utilice el siguiente mandato para crear la instancia. Escriba el mandato en una línea.  Sistemas operativos Linux

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
tsminst1 tsminst1
```

Recuerde: A partir de este momento, utilice este ID de nuevo usuario al configurar el servidor IBM Spectrum Protect. Cierre la sesión del ID de usuario `root` e inicie sesión con el nuevo ID de usuario de la instancia.

2. Cambie el directorio predeterminado de la base de datos para que sea la misma que el directorio de instancia del servidor. Si tiene varios servidores, inicie sesión en el ID de la instancia para cada servidor. Emita este mandato:

```
db2 update dbm cfg using dftdbpath directorio_instancia
```

Por ejemplo, si `directorio_instancia` es el ID del usuario de la instancia:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Modifique la vía de acceso a biblioteca para utilizar la versión del IBM Global Security Kit (GSKit) que está instalada con el servidor. En los siguientes ejemplos, `server_bin_directory` es un subdirectorio del directorio de instalación del servidor. Por ejemplo, `/opt/tivoli/tsm/server/bin`.
  - Debe actualizar los archivos siguientes para establecer la vía de acceso a biblioteca cuando se inicia DB2 o el servidor:




Ejemplo de shell Korn o bash:

```
directorio_inicio_usuarios_instancia/sqllib/userprofile
```


Ejemplo de C shell:

```
directorio_inicio_usuarios_instancia/sqllib/usercshrc
```

- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/userprofile* (shell Bash o Korn), en una línea:  Sistemas operativos Linux


```
export LD_LIBRARY_PATH=server_bin_directory/
dbbkapi:/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

Recuerde: Las siguientes entradas deben estar en la vía de acceso a biblioteca:

- /usr/local/ibm/gsk8\_64/lib64
  - /opt/ibm/lib
  - /opt/ibm/lib64
  - /usr/lib64
- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/usercshrc* (C shell), en una línea:  Sistemas operativos Linux

```
setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:
/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

4. Cree un archivo de opciones de servidor. Consulte Linux: Configuración de comunicaciones de servidor y de cliente.

 Sistemas operativos Linux

## Linux: Configuración de comunicaciones de servidor y de cliente

---

Se crea un archivo de opciones de servidor de ejemplo predeterminado, *dsmserve.opt.smp*, durante la instalación de IBM Spectrum Protect en el directorio */opt/tivoli/tsm/server/bin*. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.

### Acerca de esta tarea

---



Asegúrese de que dispone de un directorio de instancias del servidor, como */tsminst1*, y copie el archivo de muestra a este directorio. Llame a este nuevo archivo *dsmserve.opt* y edite las opciones. Finalice esta configuración antes de inicializar la base de datos de servidor. Cada entrada de ejemplo o predeterminada del archivo de opciones de muestra es un comentario, una línea que empieza con un asterisco (\*). Las opciones no distinguen entre mayúsculas y minúsculas y se permiten uno o varios espacios en blanco entre las palabras clave y los valores.


Cuando modifique el archivo de opciones, siga estas indicaciones:

- Elimine el asterisco del principio de la línea para activar una opción.
- Puede empezar a especificar las opciones en cualquier columna.
- Escriba sólo una opción por línea. La opción debe ocupar sólo una línea.
- Si realiza varias entradas para una palabra clave, el servidor de IBM Spectrum Protect aplica la última.

Si modifica el archivo de opciones del servidor, deberá volver a arrancar el servidor para que los cambios surtan efecto.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- TCP/IP Versión 4 o Versión 6
- Memoria compartida
- capa de sockets seguros (SSL)  
Consejo: Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.
-  Sistemas operativos LinuxLinux: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos LinuxLinux: Establecimiento de opciones de memoria compartida  
Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.

-  Sistemas operativos Linux Linux: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## Linux: Establecimiento de opciones de TCP/IP

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea


Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.


```
commmethod tcpip
tcpport 1500
tcpwindowsize 0
tcpnodelay yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPORT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.

 Sistemas operativos Linux TCPWINDOWSIZE

 Sistemas operativos Linux Especifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Puede especificar un entero de 0 a 2048. Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPOINT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## Linux: Establecimiento de opciones de memoria compartida

Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.

### Acerca de esta tarea

El siguiente ejemplo muestra un valor de memoria compartida:

```
commmethod sharedmem
shmport 1510
```

En este ejemplo, SHMPORT especifica la dirección de puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Utilice la opción SHMPORT para especificar un puerto TCP/IP diferente. La dirección de puerto predeterminada es 1510.


COMMmethod se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:

```
commmethod tcpip
commmethod sharedmem
```

 Sistemas operativos Linux Es posible que reciba el siguiente mensaje del servidor al utilizar la memoria compartida:

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error de msgget (2), número de error = 28
```

El mensaje significa que se debe crear una cola de mensajes pero se superará el límite de sistema para el número máximo de colas de mensajes (MSGMNI).

 Sistemas operativos Linux Para averiguar el número máximo de colas de mensajes (MSGMNI) en el sistema, emita el mandato siguiente:

```
cat /proc/sys/kernel/msgmni
```

Para aumentar el valor de MSGMNI en el sistema, emita el mandato siguiente:

```
sysctl -w kernel.msgmni=n
```

siendo **n** el número máximo de colas de mensajes que desea que el sistema admita.

## Linux: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.

## Linux: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.


Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  Sistemas operativos Linux

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Inicialización de una instancia del servidor

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es `/tsminst1`, emita los mandatos siguientes:  Sistemas operativos Linux

```
cd /tsminst1
dsmerv format dbdir=/tsmdb001 activelogsiz=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

 Sistemas operativos Linux Consejo: Si DB2 no se inicia después de emitir el mandato DSMSERV FORMAT, puede que tenga que inhabilitar la opción de montaje NOSUID del sistema de archivos. Si esta opción está establecida en el sistema de archivos que contiene el directorio de propietario de instancia de DB2, o en cualquiera de los sistemas de archivos que contienen la base de datos

de DB2 o registros activos, registros de archivos, registros de migración tras error o registros duplicados, la opción debe estar inhabilitada para iniciar el sistema.

Después de inhabilitar la opción NOSUID, vuelva a montar el sistema de archivos y después inicie DB2 emitiendo el siguiente mandato:

```
db2start
```


#### Información relacionada:

DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)

## Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos


Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

### Acerca de esta tarea

 Sistemas operativos Linux Comenzando con IBM Spectrum Protect V7.1, ya no es necesario establecer la contraseña de API durante una configuración manual del servidor. Si establece la contraseña de API durante el proceso de configuración manual, los intentos para hacer una copia de seguridad de la base de datos pueden fallar.

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos BACKUP DB o RESTORE DB.

Atención: Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 Sistemas operativos Linux En los siguientes mandatos, sustituya los valores de ejemplo por los valores reales. Los ejemplos utilizan `tsminst1` para el ID de usuario de instancia del servidor, `/tsminst1` para el directorio de instancia del servidor, y `/home/tsminst1` como directorio de inicio de usuarios de instancia del servidor.

1. Establezca la configuración de la variable de entorno de IBM Spectrum Protect para la instancia de la base de datos:

- Inicie la sesión utilizando el ID de usuario `tsminst1`.
- Cuando el usuario `tsminst1` inicia sesión, asegúrese de que el entorno de DB2 esté debidamente inicializado. El entorno de DB2 se inicializa ejecutando el script `/home/tsminst1/sqllib/db2profile`, que normalmente se ejecuta de forma automática desde el perfil del ID de usuario. Asegúrese de que el archivo `.profile` existe en el directorio de inicio de los usuarios de instancia, por ejemplo `/home/tsminst1/.profile`. Si `.profile` no ejecuta el script `db2profile`, agregue las siguientes líneas:

```
Si [-f /home/tsminst1/sqllib/db2profile]; entonces
 . /home/tsminst1/sqllib/db2profile
fi
```

c. En el archivo directorio\_instancia/sqllib/userprofile, añada las líneas siguientes:

```
DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
DSMI_DIR=directorio_bin_servidor/dbbkapi
DSMI_LOG=directorio_instancia_servidor
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

donde:

- `directorio_instancia` es el directorio de inicio del usuario de instancia de servidor.
- `directorio_instancia_servidor` es el directorio de instancia de servidor.
- `directorio_bin_servidor` es el directorio bin de servidor. La ubicación predeterminada es `/opt/tivoli/tsm/server/bin`.

En el archivo directorio\_instancia/sqllib/usercshrc, añada las líneas siguientes:

```
setenv DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
setenv DSMI_DIR=directorio_bin_servidor/dbbkapi
setenv DSMI_LOG=directorio_instancia_servidor
```

2. Cierre la sesión y vuelva a iniciar la sesión como `tsminst1` o emita este mandato:

```
. ~/.profile
```

Consejo: Asegúrese de que especifica un espacio en blanco después del primer carácter de punto (.)

3. Cree el archivo que se denomine `tsmdbmgr.opt` en el directorio `instancia_servidor`, que se encuentra en el directorio `/tsminst1` en este ejemplo, y añada la línea siguiente:

```
SERVERNAME TSMDBMGR_TSMINST1
```


Recuerde: El valor para `SERVERNAME` debe ser coherente en los archivos `tsmdbmgr.opt` y `dsm.sys`.

4. Como usuario `root`, agregue las siguientes líneas al archivo de configuración IBM Spectrum Protect API `dsm.sys`. De forma predeterminada, el archivo de configuración `dsm.sys` está en la ubicación predeterminada siguiente:
  - `directorio_bin_servidor/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

donde

- `servername` coincide con el valor de `servername` en el archivo `tsmdbmgr.opt`.
- `commethod` especifica la API de cliente que se utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Este valor puede ser `tcpip` o `sharedmem`. Para obtener más información sobre la memoria compartida, consulte el paso 5.
- `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
- `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmserv.opt`.
- `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.
- `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Para asegurarse de que se puede hacer copia de seguridad de la base de datos, este valor debe ser `$_TSMDBMGR_$$`.

 **Sistemas operativos Linux** Atención: No agregue la opción `PASSWORDACCESS generate` al archivo de configuración de `dsm.sys`. Esta opción puede causar que la copia de seguridad de la base de datos falle.

5. Opcional: configura el servidor en el cual realizar la copia de seguridad mediante el uso de una memoria compartida. De esta manera, podría reducir la carga del procesador y mejorar la capacidad. Realice los siguientes pasos:
  - a. Revise el archivo `dsmserv.opt`. Si las líneas siguientes no están en el archivo, añádalas:

```
commmethod sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

- b. En el archivo de configuración `dsm.sys`, localice las siguientes líneas:

```
commmethod tcpip
tcpserveraddr localhost
tcpport número_puerto
```

Reemplace las líneas especificadas con las siguientes líneas:

```
commmethod sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

## Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor

---


Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

### Acerca de esta tarea

---

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione

la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.


 Sistemas operativos Linux Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.

Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

## Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos Linux Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancia del servidor.

Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `/opt/tivoli/tsm/server/bin`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.

- a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```


4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.

### Información relacionada:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 [Sistemas operativos Linux](#)

## Linux: Inicio de la instancia de servidor


---

Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario `root`.

### Antes de empezar

---


Asegúrese de establecer los permisos de acceso y los límites de usuario correctamente.

 Sistemas operativos Linux Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).

### Acerca de esta tarea

---

Al iniciar el servidor utilizando el ID de usuario de la instancia, se simplifica el proceso de configuración y se evitan posibles problemas. Sin embargo, en algunos casos, es posible que sea necesario iniciar el servidor con el ID de usuario `root`. Por ejemplo, es posible que desee utilizar el ID de usuario `root` para garantizar que el servidor pueda acceder a determinados dispositivos. Puede configurar el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia o el ID de usuario `root`.


 Sistemas operativos Linux Si necesita completar un mantenimiento o tareas de reconfiguración, inicie el servidor en la modalidad de mantenimiento.

## Procedimiento

---


Para iniciar el servidor, realice una de las siguientes acciones:


- Inicie el servidor haciendo uso del ID de usuario de la instancia.


 Sistemas operativos Linux Para obtener las instrucciones, consulte Inicio del servidor desde el ID del usuario de la instancia .

- Inicie el servidor utilizando el ID de usuario root.


Para obtener instrucciones sobre cómo autorizar a los ID de usuarios root a iniciar el servidor, consulte Autorización de los ID de usuario root para iniciar el servidor (V7.1.1). Para obtener instrucciones sobre cómo iniciar el servidor utilizando el ID de usuario root, consulte el apartado Inicio del servidor desde el ID de usuario root (V7.1.1).

-  Sistemas operativos Linux Inicie el servidor automáticamente.

 Sistemas operativos Linux Para obtener instrucciones, consulte Linux: Inicio automático de los servidores en sistemas Linux.

-  Sistemas operativos Linux Inicie el servidor en modalidad de mantenimiento.

Para obtener instrucciones, consulte Linux: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos Linux

## Linux: Comprobación de los derechos de acceso y límites de usuario

---

Antes de iniciar el servidor, compruebe los derechos de acceso y límites de usuario.

### Acerca de esta tarea

---

Si no verifica los límites de usuario, conocidos también como *límitesu*, podría experimentar inestabilidad del servidor o una falla del servidor al responder. También debe verificar el límite en todo el sistema para ver el número máximo de archivos abiertos. El límite de todo el sistema debe ser mayor que o equivalente al límite de usuario.

## Procedimiento


---

1. Compruebe que el ID del usuario de la instancia del servidor tenga autorizaciones para iniciar el servidor.
2. Para la instancia del servidor que piensa iniciar, asegúrese que tiene la autoridad para leer y escribir archivos en el directorio de la instancia del servidor. Compruebe que el archivo `dsmserv.opt` existe en el directorio de la instancia del servidor y de que el archivo incluye parámetros para la instancia del servidor.
3. Si el servidor está conectado a una unidad de cinta, cambiador de recursos o dispositivo de soporte extraíble y piensa iniciar el servidor mediante el uso del ID del usuario de la instancia, otorgue acceso de lectura/escritura al ID de usuario de instancias para esos dispositivos. Para establecer los permisos, realice una de las siguientes acciones:
  - Si el sistema está dedicado a IBM Spectrum Protect y solo el administrador de IBM Spectrum Protect tiene acceso, haga que el archivo especial del dispositivo sea grabable para todos los usuarios. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod +w /dev/rmtX
```
  - Si el sistema cuenta con varios usuarios, puede restringir el acceso si hace que el ID de usuario de la instancia de IBM Spectrum Protect sea el propietario de los archivos especiales de dispositivo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod u+w /dev/rmtX
```
  - Si se están ejecutando varias instancias de usuario en el mismo sistema, cambie el nombre de grupo, por ejemplo TAPEUSERS, y añada cada ID de usuario de instancia IBM Spectrum Protect a dicho grupo. A continuación cambie la propiedad de los archivos especiales de dispositivo para que pertenezcan al grupo TAPEUSERS y haga que sean grabables para el grupo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod g+w /dev/rmtX
```

4.  Sistemas operativos Linux Si está usando el controlador de dispositivos IBM Spectrum Protect y el programa de utilidad `autoconf`, use la opción `-a` para otorgar acceso de lectura/escritura al ID de usuario de la instancia.



5.  Sistemas operativos Linux Para evitar fallas del servidor, durante la interacción con DB2, ajuste los parámetros de kernel.
-  Sistemas operativos Linux Para obtener instrucciones sobre cómo ajustar los parámetros de kernel, consulte Linux: Ajuste de parámetros del kernel en sistemas Linux.
6. Compruebe los siguientes límites de usuario con base en los lineamientos de la tabla.

Tabla 1. Valores del límite (no límite) de usuario

Tipo de límite de usuario	Valor recomendado	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	Ilimitada	<code>ilimitado -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	Ilimitada	<code>ulimit -Hd</code>
Tamaño de archivo máximo	Ilimitada	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	65536	<code>ulimit -Hn</code>
La cantidad máxima de tiempo del procesador en segundos	Ilimitada	<code>ilimitado -Ht</code>


Para modificar los límites de usuario, siga las instrucciones en la documentación del sistema operativo.

Consejo: Si planea iniciar el servidor automáticamente haciendo uso de un script, puede establecer los límites de usuario en el script.

7. Asegúrese de que el límite de usuario de procesos de usuario máximos (el valor de `nproc`) se establece en el valor mínimo sugerido de 16384.
- Para verificar el límite de usuario actual, emita el mandato `ulimit -Hu` utilizando el ID de usuario de instancia. Por ejemplo:


```
[user@Machine ~]$ ulimit -Hu
16384
```

- Si el límite de procesos máximos del usuario no se establece en 16384, establezca el valor en 16384.

 Sistemas operativos Linux Añada la siguiente línea al archivo `/etc/security/limits.conf`:

```
id_usuario_instancia - nproc 16384
```

donde `id_usuario_instancia` especifica el ID de usuario de instancia de servidor.

 Sistemas operativos Linux Si el servidor está instalado en el sistema operativo Red Hat Enterprise Linux 6, establezca el límite de usuario al editar el archivo `/etc/security/limits.d/90-nproc.conf` en el directorio `/etc/security/limits.d`. Este archivo sustituye a los valores del archivo `/etc/security/limits.conf`.

Consejo: El valor predeterminado del límite de usuario de los procesos máximos de usuario cambió en algunas distribuciones y versiones del sistema operativo Linux. El valor predeterminado es 1024. Si no cambia el valor al valor mínimo sugerido de 16384, el servidor podría fallar o colgarse.

 Sistemas operativos Linux

## Linux: Inicio del servidor con el ID de usuario de la instancia

Para iniciar el servidor desde el ID de usuario de la instancia, inicie sesión con el ID de usuario de la instancia y emita el mandato correspondiente desde el directorio de la instancia del servidor.

### Antes de empezar

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para obtener instrucciones, consulte Linux: Comprobación de los derechos de acceso y límites de usuario.

### Procedimiento

- Inicie sesión en el sistema donde instalado IBM Spectrum Protect utilizando el ID de usuario de instancia para el servidor.
- Si no tiene un perfil de usuario que ejecuta el script de `db2profile`, emita el siguiente mandato:

```
. /home/tsminst1/sqllib/db2profile
```

Consejo: Para obtener instrucciones sobre cómo actualizar el script de inicio de sesión de ID de usuario para ejecutar el script `db2profile` automáticamente, consulte la documentación de DB2.


- Inicie el servidor emitiendo el siguiente mandato en una línea desde el directorio de instancia del servidor:

 Sistemas operativos Linux




```
usr/bin/dsmserve
```

Consejo: El mandato se ejecuta en primer plano para que pueda configurar un ID de administrador y conectarlo con la instancia del servidor.

 Sistemas operativos Linux Por ejemplo, si el nombre de la instancia del servidor es `tsminst1` y el directorio de la instancia de servidor es `/tsminst1`, puede iniciar la instancia emitiendo los mandatos siguientes:

```
cd /tsminst1
. ~/sqllib/db2profile
/usr/bin/dsmserve
```

 Sistemas operativos Linux

## Linux: Inicio automático de los servidores en sistemas Linux

---

Para iniciar automáticamente un servidor en un sistema operativo Linux, utilice el script `dsmserve.rc`.

### Antes de empezar

---

Asegúrese de que los parámetros de kernel están configuradas correctamente. Si desea instrucciones, consulte Ajuste de parámetro de kernel para sistemas Linux.

Asegúrese de que la instancia de servidor se ejecuta bajo el ID de usuario del propietario de instancia.

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para ver las instrucciones, consulte Verificación de los derechos de acceso y límites de usuario.

### Acerca de esta tarea

---

El script `dsmserve.rc` está en el directorio de instalación del servidor, por ejemplo, `/opt/tivoli/tsm/server/bin`.

El script `dsmserve.rc` se puede usar para iniciar manualmente un servidor o para iniciar automáticamente el servidor al agregar entradas al directorio `/etc/rc.d/init.d`. El script funciona con los programas de utilidad Linux como por ejemplo `CHKCONFIG` y `SERVICE`.

### Procedimiento

---

Para cada instancia del servidor que desee iniciar automáticamente, realice los pasos siguientes:

1. Coloque una copia del script `dsmserve.rc` en el directorio `/init.d`, por ejemplo, `/etc/rc.d/init.d`.

Asegúrese de cambiar solo la copia del script. No modifique el script original.

2. Cambie el nombre de la copia del script de modo que coincida con el nombre del propietario de la instancia de servidor, por ejemplo, `tsminst1`.

El script se ha creado suponiendo que el directorio de instancia de servidor es *directorio\_raíz/tsminst1*, por ejemplo: `/home/tsminst1/tsminst1`.

3. Si el directorio de instancia de servidor no es *directorio\_raíz/tsminst1*, localice la línea siguiente en la copia del script:

```
instance_dir="${instance_home}/tsminst1"
```

Cambie la línea para que apunte al directorio de instancia de servidor, por ejemplo:

```
instance_dir="/tsminst1"
```

4. En la copia de script, localice la línea siguiente:

```
pidfile: /var/run/dsmserve_instancename.pid
```

Cambie el valor de nombre de instancia por el nombre del propietario de instancia de servidor. Por ejemplo, si el propietario de instancia de servidor es `tsminst1`, actualice la línea como se muestra:

```
pidfile: /var/run/dsmserve_tsminst1.pid
```

5. Configure el nivel de ejecución en el que el servidor se inicia automáticamente. Mediante el uso de herramientas como el programa de utilidad `CHKCONFIG`, especifique un valor que corresponda a una modalidad multiusuario, con la conexión de redes activada. Generalmente, el nivel de ejecución que se utilizará es 3 o 5, en función del sistema operativo y de su configuración.

Para obtener más información acerca de la modalidad multiusuario y los niveles de ejecución, consulte la documentación del sistema operativo.

6. Para iniciar o detener el servidor, emita uno de los mandatos siguientes:

- o Para iniciar el servidor:

```
service tsminst1 start
```

- o Para detener el servidor:

```
service tsminst1 stop
```

## Ejemplo


---


Este ejemplo utiliza los siguientes valores:

- El propietario de instancia es `tsminst1`.
- El directorio de instancia de servidor es `/home/tsminst1/tsminst1`.
- La copia de script `dsmserve.rc` se denomina `tsminst1`.
- El programa de utilidad `CHKCONFIG` se utiliza para configurar que el script se inicie a los niveles de ejecución 3, 4 y 5.

```
cp /opt/tivoli/tsm/server/bin/dsmserve.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserve_instancename.pid/dsmserve_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

### Referencia relacionada:

 Script de inicio del servidor: `dsmserve.rc`

 Sistemas operativos Linux

## Linux: Inicio del servidor en modalidad de mantenimiento

---

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad `DSMSERV` con el parámetro `MAINTENANCE`.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, `dsmserve.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

### Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserve maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

## Qué hacer a continuación

---

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## Linux: Detención del servidor

---


Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

### Acerca de esta tarea


---

Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:

```
halt
```

 Sistemas operativos Linux Si no se puede conectar al servidor con un cliente administrativo y desea detener el servidor, debe cancelar el proceso utilizando el mandato kill con el número del ID de proceso (pid). El pid se muestra en la inicialización. **Importante:** Antes de emitir el mandato kill, asegúrese de que conoce el ID de proceso correcto del servidor IBM Spectrum Protect. El archivo `dsmserv.v6lock`, en el directorio desde el cual se está ejecutando el servidor, se puede usar para identificar el ID de proceso del proceso que desea detener. Para mostrar el archivo, especifique:

```
cat /instance_dir/dsmserv.v6lock
```

 Sistemas operativos Linux Emita el siguiente mandato para detener el servidor:

```
kill -23 dsmserv_pid
```

donde `dsmserv_pid` es el número de ID del proceso.

## Linux: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

### Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

### Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

### Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

## Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

## Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

## Ejemplo

---

Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:


```
set dbrecovery dbback
```

## Linux: Ejecución de varias instancias de servidor en un solo sistema

---

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.

Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.


 Sistemas operativos LinuxEl conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos de Linux: Creación de una instancia del servidor para cada instancia nueva, incluida la creación del nuevo usuario de la instancia.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.

Puede actualizar directamente de V7.1 a V8.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.3 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

### Tareas relacionadas:

 Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## Linux: Supervisión del servidor

---

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## Procedimiento

---

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la

cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de espacio de las anotaciones activas, pero durante poco tiempo.
  - Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.
- Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tarden más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

## 2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible.

Recuerde: Si el registro de archivado y el registro de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.

Probablemente observará el siguiente patrón:

- a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
- b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.
- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## Linux: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.3 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.3, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado Linux: Revertir de la versión 8.1.3 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:



```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación. La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7.  Sistemas operativos Linux Conéctese como usuario root.
8. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
9.  Sistemas operativos Linux Cambie al directorio donde situó el archivo ejecutable y complete los pasos siguientes.  
Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.

- a. Cambie los permisos de archivo emitiendo el siguiente mandato:

```
chmod a+x 8.x.x.x-IBM-SPSRV-plataforma.bin
```

- donde *plataforma* indica la arquitectura en la que se va a instalar IBM Spectrum Protect.
- b. Emita el siguiente mandato para extraer los archivos de instalación:

```
./8.x.x.x-IBM-SPSRV-plataforma.bin
```

10. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.

Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.

Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

Asistente de instalación

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect en modalidad de consola

Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.

## Resultados

---

Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos Linux/var/ibm/InstallationManager/logs

## Linux: Reverta de la versión 8.1.3 a un servidor anterior

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

### Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:

- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

### Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.3 al 8.1.2 o del 8.1.3 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.


### Pasos para recuperar la versión anterior del servidor


---

## Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

## Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato: Sistemas operativos Linux

```
dsmserv removedb tsmdl
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado Linux: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.3. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato: Sistemas operativos Linux

```
./dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.
7. Restablezca la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - o Archivo de configuración de dispositivos
  - o Archivo histórico de volúmenes
  - o El archivo de opciones de servidor (generalmente dsmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.3, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de seguridad de la base de datos. Utilice el mandato RESTORE VOLUME.  
Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:

```
audit volume nombre_volumen fix=yes
```
11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

---

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.3, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.3.

## Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.3:



- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.3. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

## Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:
  - Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.3.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro REUSEDELAY para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.3. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.3, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.3.

## Linux: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect

Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.


### Finalidad

Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.

Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.

Tabla 1. Mandatos de DB2

Man dato	Descripción	Ejemplo
----------	-------------	---------

Man dato	Descripción	Ejemplo
db2i crt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia.</p> <p>Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p> <p> Sistemas operativos LinuxEste programa de utilidad está en el directorio DB2DIR/instance, donde DB2DIR representa la ubicación donde se instala la versión actual del sistema de base de datos de DB2.</p>	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre>/opt/tivoli/ts m/db2/instance / db2icrt -a server -u nombre_instanc ia nombre_instanc ia</pre>
db2s et	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> <pre>db2set</pre>
CAT ALO G DAT ABASE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	<p>Catalogue la base de datos:</p> <pre>db2 catalog database tsmdb1</pre>
CON NEC T TO DAT ABASE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	<p>Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:</p> <pre>db2 connect to tsmdb1</pre>
GET DAT ABASE CON FIG URATIO N	<p>Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico.</p> <p>Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .</p>	<p>Muestre la información de configuración para un alias de base de datos:</p> <pre>db2 get db cfg for tsmdb1</pre> <p>Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.</p> <pre>db2 get db config for tsmdb1 show detail</pre>

Man dato	Descripción	Ejemplo
GET DAT ABA SE MAN AGE R CON FIG URA TIO N	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEA LTH SNA PSH OT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsmdb1
GRA NT (Aut oriza cion es de base de dato s)	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser
RUN STAT S	Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.  Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.  Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.  Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.	Actualice las estadísticas en una única tabla.  db2 runstats on table SCHEMA_NAME.TA BLE_NAME with distribution and sampled detailed indexes all
SET SCH EMA	Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2. Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.	Establezca el esquema para IBM Spectrum Protect:  db2 set schema tsmdb1
STA RT DAT ABA SE MAN AGE R	Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor. Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.	Inicie el gestor de base de datos:  db2start

Man dato	Descripción	Ejemplo
STO P DAT ABA SE MAN AGE R	<p>Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.</p> <p>Este mandato no es válido en un cliente.</p> <p>El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Detenga el gestor de base de datos:</p> <pre>db2 stop dbm</pre>

## Linux: Desinstalar IBM Spectrum Protect

Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.
- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

### Acerca de esta tarea

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- **Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico**  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.
- **Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola**  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- **Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa**  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- **Linux: Desinstalación e instalación de IBM Spectrum Protect**  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- **Linux: Desinstalación de IBM Installation Manager**  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

### Qué hacer a continuación


Consulte Linux: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento

1. Inicie el Installation Manager.

 Sistemas operativos Linux En el directorio en donde se encuentra instalado Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:

```
./IBMIM
```

2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.


## Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola

---



Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.

### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Linux/eclipse/tools

Por ejemplo:

-  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio herramientas, emita el siguiente mandato:
  -  Sistemas operativos Linux ./imcl -c
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique N para Siguiente.
6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
7. Especifique N para Siguiente.
8. Escriba U para Desinstalar.
9. Escriba F para Finalizar.

## Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

---

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.

### Antes de empezar

---


Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.



Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Linux/eclipse/tools

Por ejemplo:

-  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio herramientas, emita el siguiente mandato, donde `archivo_respuestas` representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:  
 Sistemas operativos Linux  

```
./imcl -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos Linux

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## Linux: Desinstalación e instalación de IBM Spectrum Protect


---

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.

### Acerca de esta tarea


---

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos Linux Realice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:


```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:

 Sistemas operativos Linux


```
db2 attach to instance_name
db2 get dbm cfg show detail
db2 detach
```

Mantenga un registro de la ruta de base de datos para cada instancia.

3. Desinstale IBM Spectrum Protect. Consulte el apartado Linux: Desinstalar IBM Spectrum Protect.
4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten las credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estas credenciales utilizando la variable `INSTANCE_CRED`. Puede encontrar el archivo de instancias en la siguiente ubicación:
  - o  Sistemas operativos Linux/etc/tivoli/tsm/instanceList.obj
5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado Linux: Instalación de los componentes de servidor.

Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- a. Vuelva a crear las instancias de servidor. Consulte el apartado Linux: Creación de una instancia del servidor. Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- b. Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos Linux

```
db2 catalog database tsmdb1
db2 attach to instance_name
db2 update dbm cfg using dftdbpath instance_directory
db2 detach
```

- c.  Sistemas operativos Linux Compruebe que la instancia de servidor se haya creado correctamente. Emita este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```

Si figura TSMDDB1 puede iniciar el servidor.

## Linux: Desinstalación de IBM Installation Manager


---

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

## Antes de empezar

---

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.

 Sistemas operativos Linux Para ver los paquetes instalados, emita el mandato siguiente desde una línea de mandatos:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

## Procedimiento

---

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos Linux

1. Abra una línea de mandatos y cambie el directorio a `/var/ibm/InstallationManager/uninstall`.
2. Emita el mandato siguiente:

```
./uninstall
```

Restricción: Debe haber iniciado sesión en el sistema utilizando el ID de usuario `root`.

## Windows: Instalación del servidor

---


La instalación del servidor incluye la planificación, instalación y configuración inicial.

- Windows
- Windows: Planificación para instalar el servidor  
Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- Windows: Instalación de los componentes de servidor  
Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Windows: Primeros pasos tras instalar IBM Spectrum Protect  
Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.
- Windows: Instalación de un fixpack de servidor de IBM Spectrum Protect  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.
- Windows: Revertir de la versión 8.1.3 a un servidor anterior  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- Windows: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- Windows: Desinstalar IBM Spectrum Protect  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## Windows: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.

- Windows: Qué debe saber primero  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- Windows: Planificación de rendimiento óptimo  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  Sistemas operativos Windows Windows: Requisitos mínimos del sistema para sistemas Windows  
El servidor puede requerir una gran cantidad de memoria, ancho de banda de red y recursos de procesador. En muchos casos, el servidor funciona mejor cuando las otras aplicaciones no están instaladas en el mismo sistema.


- **Windows: IBM Installation Manager**  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- **Windows: Hojas de trabajo para planificar detalles para el servidor**  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- **Windows: Planificación de la capacidad**  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.
- **Windows: Prácticas más adecuadas de denominación del servidor**  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- **Windows: Directorios de instalación**  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.


## Windows: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 **Sistemas operativos Windows** Restricción: No puede instalar y ejecutar el servidor de la Versión 8.1.3 en un sistema que ha tenga DB2 instalado en el mismo, tanto si DB2 se ha instalado por sí mismo o como parte de alguna otra aplicación. El servidor de la V8.1.3 necesita que se instale y utilice la versión de DB2 que está empaquetada con el servidor de la V8.1.3. No puede haber ninguna otra versión de DB2 en el sistema.

 **Sistemas operativos Windows** Puede instalar el servidor en IBM Spectrum Protect en un controlador de dominio. Sin embargo, el servidor puede tener un uso de procesador intensivo y esto podría afectar y detener otras aplicaciones.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.3 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.

**Atención:** No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Windows: Planificación de rendimiento óptimo

---

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.

### Procedimiento

---

1. Revise **Windows: Qué debe saber primero**.
2. Revise cada una de las siguientes subsecciones.
  - **Windows: Planificación del hardware del servidor y el sistema operativo**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Windows: Planificación de discos de base de datos del servidor**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Windows: Planificación de discos de registro de recuperación del servidor**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Windows: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios**  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.




- Windows: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
- Windows: Planificación del tipo correcto de tecnología de almacenamiento  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
- Windows: Aplicación de prácticas recomendadas para la instalación del servidor  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

## Windows: Planificación del hardware del servidor y el sistema operativo

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul>	<p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p>
<p>¿Están configurados los discos para un rendimiento óptimo?</p>	<p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿El servidor tiene suficiente memoria?	<p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p>	<p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul>
¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente?	<p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>	<p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?	<p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul>
¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect?	<p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. Para obtener más información sobre el sistema de archivos preferido para su sistema operativo, consulte IBM Spectrum Protect server-supported file systems.</p>	<p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>
¿Tiene pensado configurar suficiente espacio de paginación?	<p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos Windows El espacio de paginación se configura automáticamente.</p>	

## Windows: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---------------------------------------------	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Se encuentra la base de datos en discos rápidos de baja latencia?	<p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p>	Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.
¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento?	<p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>	
Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?	<p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>	
Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?	Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.	El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p>	<p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <code>DB2_PARALLEL_IO</code> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <code>DB2_PARALLEL_IO</code>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <code>DB2_PARALLEL_IO</code>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>	<p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>	
<p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>	<p>La profundidad de cola predeterminada suele ser demasiado baja.</p>	<p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>

## Windows: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos?	Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.	La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.
¿Se encuentran los registros en discos con memoria caché de escritura no volátil?	La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.	
¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?	Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.  Registro activo El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.  Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.  Registro de archivos El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo.	<ul style="list-style-type: none"> <li>Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>
¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?	El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.	Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.  Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande.
Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?	Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro. <ul style="list-style-type: none"> <li>Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>Utilice la duplicación en el hardware del sistema de disco.</li> </ul>	Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.  Para obtener más información, consulte Configuración y ajuste del registro de recuperación.

## Windows: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p>	<p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$	<p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>	<p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul>	<p>Requisitos de memoria</p>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>	<p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p>	<p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>	<p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>	<p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p>	<p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>	<p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p>
<p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>	<p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>	<ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>



Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha asignado suficiente espacio de almacenamiento para la base de datos?</p>	<p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>	
<p>¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?</p>	<p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol>	<p>Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?	<p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p>	<p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad?	<p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>	<ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>
¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?	<p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>	<p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?	<p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>	Para obtener más información, consulte la opción de cliente enablededup.
¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?	<p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>	
¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?	<p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul>	

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha seleccionado el tipo apropiado de almacenamiento local?</p>	<p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul>	

## Windows: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---------------------------------------------	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo?	<p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p>	Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.
¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?	Utilice más memoria caché para un mejor rendimiento.	
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?	Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.	Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario.
Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?	<p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>	<p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>
Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?	Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.	Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?</p>	<p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p>	<p>Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.</p>
<p>En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?</p>	<p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>	<p>Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.</p>
<p>¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?</p>	<p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>	<p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul>

## Windows: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento

Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

<b>Tipo de tecnología de almacenamiento</b>	<b>Base de datos</b>	<b>Registro activo</b>	<b>Registro de archivado y registro de migración tras error de archivado</b>	<b>Agrupaciones de almacenamiento</b>
<b>Unidad de estado sólido (SSD)</b>	<p>Coloque la base de datos en SSD en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>	<p>Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>
<p><b>Disco de alto rendimiento con las siguientes características:</b></p> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.</p>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.</p>	<p>Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.</p>	<p>Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.</p>

Tipo de tecnología de almacenamiento	Base de datos	Registro activo	Registro de archivado y registro de migración tras error de archivado	Agrupaciones de almacenamiento
<b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>Disco de 10.000 rpm</li> <li>Interfaz Fibre Channel o SAS</li> </ul>	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aísle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aísle estos registros de la base de datos y registro activo.	Utilice disco de rendimiento medio o rendimiento alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>Los datos se leen con frecuencia.</li> <li>Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aísle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.
<b>SATA, almac. adjunto de red</b>	No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.	No utilice este almacenamiento para el registro activo.	El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.	Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>Los datos se leen con poca frecuencia.</li> </ul>
<b>Cinta y cinta virtual</b>				Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.

## Windows: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

Práctica recomendada	Más información
----------------------	-----------------



<b>Práctica recomendada</b>	<b>Más información</b>
<p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p>	<p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>
<p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>
<p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>	<p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>
<p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>	<p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>
<p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>	<p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>

Práctica recomendada	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores.	<p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p>
Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.	<p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>○ Ajuste de la planificación para las operaciones diarias</li> <li>○ Lista de comprobación para la configuración de servidor</li> </ul>
Supervise las operaciones de forma constante.	<p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento.</p> <p>Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>

## Windows: Requisitos mínimos del sistema para sistemas Windows

El servidor puede requerir una gran cantidad de memoria, ancho de banda de red y recursos de procesador. En muchos casos, el servidor funciona mejor cuando las otras aplicaciones no están instaladas en el mismo sistema.

## Requisitos de software y de hardware de la instalación del servidor de IBM Spectrum Protect

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

## Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Windows: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Hardware	Un procesador AMD64 o Intel EMT-64

Tipo de hardware	Requisitos de hardware
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• Al menos, 7,5 GB de almacenamiento de disco libre para una instalación típica</li> <li>• 60 MB en el espacio de directorio temporal</li> <li>• Una partición de 2 GB en la unidad C:\</li> <li>• 300 MB en el directorio de instancias</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Windows: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos mínimos de software necesarios para un servidor en un sistema Windows.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	<p>Uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2012: Standard, Enterprise o Datacenter Edition (64 bits)</li> <li>• Microsoft Windows Server 2012 R2 (64 bits)</li> <li>• Microsoft Windows Server 2016</li> </ul>
Protocolo de comunicaciones	<p>Al menos uno de los siguientes protocolos de comunicación (instalado de forma predeterminada con los sistemas operativos Windows actuales):</p> <ul style="list-style-type: none"> <li>• Named Pipes</li> <li>• TCP/IP Versión 4 o Versión 6</li> </ul>

Tipo de software	Requisitos mínimos de software
Controladores de dispositivo	<p>El controlador de dispositivo de paso directo IBM Spectrum Protect que se requiere para dispositivos y bibliotecas de cintas que no sean de IBM®. El controlador de dispositivos nativo de Windows se recomienda para las bibliotecas de cintas y controladores de cintas. De lo contrario, se puede usar el controlador de dispositivo kernel IBM Spectrum Protect.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p>
Otro software	<p>Windows 2012, Windows 2012 R2 y Windows 2016 requieren que .NET Framework 3.5 esté instalado y habilitado.</p> <p>Se deben desactivar las siguientes políticas de Control de la cuenta de usuario:</p> <ul style="list-style-type: none"> <li>• Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada</li> <li>• Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador</li> </ul> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Windows: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager
- Oferta de IBM Spectrum Protect

### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es `IBM Installation Manager`.

### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.


### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## Windows: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarle a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

 **Sistemas operativos Windows** Restricción: Si está utilizando una tabla de asignación de archivos (FAT o FAT32) o un formato NTFS (New Technology File System), no puede especificar el directorio raíz de dicho sistema como la ubicación de un directorio de base de datos o un directorio de registro. En su lugar, debe crear uno o varios subdirectorios dentro del directorio raíz. A continuación, cree los directorios de bases de datos y directorios de registros dentro de los subdirectorios.

Elemento	Espacio necesario	Número de directorios	Ubicación de los directorios
La base de datos			
Registro activo			
Registro de archivos			
Opcional: duplicado de registro para el registro activo			
Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado)			

Elemento	Nombres e ID de usuario	Ubicación
El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect		
El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia		
El nombre de instancia de la base de datos		
El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor)		
El nombre del servidor; utilice un nombre exclusivo para cada servidor		

## Windows: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- **Windows: Estimación de los requisitos de espacio para la base de datos**  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.
- **Windows: Requisitos de espacio del registro de recuperación**  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- Windows: Supresión de archivos de retrotracción de instalación  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Windows: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- Windows: Estimación de los requisitos de espacio de base de datos en función del número de archivos  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- Windows: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- Windows: El gestor de bases de datos y el espacio temporal  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## Windows: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.
- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.

En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

---

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:

$$500 * 3.5 = 1.7 \text{ TB}$$

## Resultados

---

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrecer acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

Tamaño de la base de datos	Requisito mínimo de espacio temporal
< 500 GB	50 GB
≥ 500 GB y < 1 TB	100 GB
≥ 1 TB y < 1,5 TB	150 GB
≥ 1,5 y < 2 TB	200 GB
≥ 2 y < 3 TB	250 - 300 GB
≥ 3 y < 4 TB	350 - 400 GB

## Windows: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## Windows: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.
- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G



de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.

- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## Windows: Requisitos de espacio del registro de recuperación

---

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- Windows: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- Windows: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- Windows: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## Windows: Espacio del registro activo y archivado

---

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:

- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.
- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.

- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- Windows: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

número de clientes x archivos almacenados durante cada transacción  
x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.

Elemento	Valores de ejemplo	Descripción
Espacio de registro necesario para cada archivo	3053 bytes	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	19,5 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p>(300 cliente x 4096 archivos almacenados durante cada transacción x 3053 bytes para cada archivo) ÷ 1.073.741.824 bytes = 3,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p>3,5 + 16 = 19,5 GB</p>
Registro de archivado: Tamaño recomendado	58,5 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p>3,5 x 3 = 10,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p>10,5 + 48 = 58,5 GB</p>
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

Elemento	Valores de ejemplo	Descripción
----------	--------------------	-------------

Elemento	Valores de ejemplo		Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	1000	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Sesiones posibles para cada cliente	3	3	El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.
Archivos almacenados durante cada transacción	4096	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3053	3053	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	26,5 GB <sup>1</sup>	51 GB <sup>1</sup>	<p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	79,5 GB <sup>1</sup>	153 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
Registro de archivado: Tamaño recomendado	60 GB <sup>1</sup>	Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:  $4 \text{ GB} \times 3 = 12 \text{ GB}$  Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:  $12 + 48 = 60 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

$300 \text{ clientes} \times 100.000 \text{ archivos por cada cliente} \times 110 \text{ bytes} = 3,1 \text{ GB}$

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## Windows: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.

La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día	60 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana	132 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

### La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

### El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

### El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

### El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La



agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.
Tamaño medio de extensiones	700 KB	700 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.
Extensiones para un determinado archivo	1.198.372 bits	6.135.667 bits	Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.  Se ha utilizado el siguiente cálculo para un objeto de 800 GB: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$  Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	1,7 GB	8,6 GB	El espacio de registro activo estimado necesario para esta transacción.

Elemento	Valores de ejemplo		Descripción
Registro activo: Tamaño total recomendado	66 GB <sup>1</sup>	79,8 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$
Registro de archivado: Tamaño recomendado	198 GB <sup>1</sup>	239,4 GB <sup>1</sup>	<p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.

Elemento	Valores de ejemplo		Descripción
Tamaño medio de extensiones	256 KB	256 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.
Extensiones para un determinado archivo	3.276.800 bits	16.777.216 bits	<p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.,276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	4,5 GB	23,4 GB	El tamaño estimado del espacio de registro activo necesario para esta transacción.
Registro activo: Tamaño total recomendado	71,6 GB <sup>1</sup>	109,4 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$

Elemento	Valores de ejemplo		Descripción
Registro de archivado: Tamaño recomendado	214,8 GB <sup>1</sup>	328,2 GB <sup>1</sup>	<p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

## Windows: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## Windows: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## Windows: Supresión de archivos de retrotracción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.
- Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

## Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.
2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.


## Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos

---



Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Windowseclipse\tools

Por ejemplo:

-  Sistemas operativos WindowsC:\Archivos de programa\IBM\Installation Manager\eclipse\tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
    -  Sistemas operativos Windowsimcl.exe -c
  3. Especifique **P** para seleccionar Preferencias.
  4. Especifique **3** para seleccionar Archivos a restaurar.
  5. Especifique **D** para Suprimir los Archivos a restaurar.
  6. Especifique **A** para Aplicar cambios y volver al menú Preferencias.
  7. Especifique **C** para salir del Menú Preferencias.
  8. Especifique **X** para Salir de Installation Manager.

## Windows: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.


### Identificador de usuario de la instancia

---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.

 Sistemas operativos Windows

## Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos es el nombre de la instancia del servidor tal y como aparece en el registro.

Por ejemplo: Server1

 Sistemas operativos Windows

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede utilizar un nombre que incluya el nombre de la instancia del servidor tal y como aparece (o aparecerá) en el registro. Los nombres de las instancias del servidor predeterminadas tienen la forma Serverx.

Por ejemplo: C:\tsm\server1

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor dsmserv.opt
- El archivo de la base de datos de la clave del servidor, cert.kdb, y los archivos .arm (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre TSMDB1, para todas las instancias del servidor. Este nombre no puede modificarse.

## Nombre de servidor

---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 Sistemas operativos Windows El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato QUERY SERVER), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.

Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.

 Sistemas operativos Windows Por ejemplo,

- TUCSON\_SERVER1
- TUCSON\_SERVER2

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos Windows f:\server1\archlog

## Windows: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

`/opt/tivoli/tsm/server/bin` es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es `/opt/tivoli/tsm/db2`.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## Windows: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.3, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Con el software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones

 Sistemas operativos Windows Deje aproximadamente entre 15 y 30 minutos para instalar un servidor V 8.1.3, utilizando esta guía.

- Windows: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- Windows: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- Windows: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## Windows: Obtener el paquete de instalación


---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos Windows

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Cambie al directorio en el que colocó el archivo ejecutable.



Importante: En el siguiente paso, los archivos se extraen al directorio actual. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.

- c. Pulse dos veces en el siguiente archivo ejecutable o introduzca el siguiente mandato en la línea de mandatos para extraer los archivos de instalación. Los archivos se extraen al directorio actual.

`nombre_paquete.exe`

donde `nombre_paquete` es como el siguiente ejemplo: `8.1.x.000-IBM-SPSRV-WindowsX64.exe`


3. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - o Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - o Windows: Instalación de IBM Spectrum Protect en modalidad de consola
  - o Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa
4. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.



### Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
-  Sistemas operativos Windows Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento



Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<ol style="list-style-type: none"><li>a. Cambie al directorio donde ha descargado el paquete.</li><li>b. Inicie el asistente de instalación emitiendo el mandato siguiente:  Sistemas operativos Windows  <code>install.bat</code>   Sistemas operativos WindowsO, en el directorio en donde se extrajeron los archivos de instalación, haga doble clic en el archivo <code>install.bat</code>.</li></ol>

### Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.

Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.

- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Windows Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos Windows Si hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe`


se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es C:\Program Files\Tivoli\TSM\device\drivers.

## Windows: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.


### Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:




- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
-  Sistemas operativos Windows Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento

Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p> <p> Sistemas operativos Windows</p> <pre>install.bat -c</pre> <p>Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique G para generar las respuestas.</p>

### Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos Windows C:\ProgramData\IBM\Installation Manager\logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Windows Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos Windows Si hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es C:\Program Files\Tivoli\TSM\device\drivers.

## Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

### Antes de empezar

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento

---


1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.

Si está utilizando el archivo `install_response_sample.xml`, añada la contraseña en la línea siguiente del archivo, donde `mypassword` representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación




Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo `update_response_sample.xml`.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor `archivo_respuestas` representa la vía de acceso del archivo de respuestas y el nombre del archivo:
  - o  Sistemas operativos Windows

```
install.bat -s -input archivo_respuestas
-acceptLicense
```

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  - o  Sistemas operativos WindowsC:\ProgramData\IBM\Installation Manager\logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos WindowsDespués de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos WindowsSi hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es `C:\Program Files\Tivoli\TSM\device\drivers`.

 Sistemas operativos Windows

## Windows: Instalación de paquetes de idioma del servidor

---

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

### Antes de empezar

---


Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.

- Windows: Idiomas locales del servidor  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- Windows: Configuración de un paquete de idiomas  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.
- Windows: Actualización de un paquete de idiomas  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## Windows: Idiomas locales del servidor

---

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 Sistemas operativos Windows Este paquete de idioma se instala automáticamente para la opción de idioma predeterminada siguiente para los mensajes de servidor y de ayuda: LANGUAGE AMENG.

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera. Puede utilizar los idiomas que se muestran:



 Sistemas operativos Windows

Tabla 1. Idiomas del servidor para Windows

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	chs
Chino, tradicional	cht
Inglés	ameng
Francés	fra
Alemán	deu
Italiano	ita
Japonés (Shift-JIS)	jpn
Coreano	kor
Portugués, de Brasil	ptb
Ruso	rus
Español	esp

 Sistemas operativos Windows Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.


## Windows: Configuración de un paquete de idiomas

---

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

### Acerca de esta tarea

---

 Sistemas operativos Windows Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo: para utilizar el entorno local `ita`, establezca la opción LANGUAGE en `ita`. Consulte Windows: Idiomas locales del servidor.

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## Windows: Actualización de un paquete de idiomas

---

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

---

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.

Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.




## Windows: Primeros pasos tras instalar IBM Spectrum Protect

---

Tras instalar la versión de 8.1.3, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

## Acerca de esta tarea

---

1. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado Windows: Creación del ID de usuario y de directorios para la instancia del servidor.
  2. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
    - Utilice el asistente de configuración, el método preferido. Consulte el apartado Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
    - Configure manualmente la nueva instancia. Consulte el apartado Windows: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
      - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte Windows: Creación de una instancia del servidor.
      - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  Sistemas operativos Windows Windows: Configuración de comunicaciones de servidor y de cliente.
      - c. Emita el mandato DSMSERV FORMAT para formatear la base de datos. Consulte el apartado Windows: Formateo de la base de datos y las anotaciones.
      - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
  3. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
  4. Inicie la instancia del servidor, si todavía no se ha iniciado.
    -  Sistemas operativos Windows Consulte el apartado Windows: Inicio de la instancia del servidor en sistemas Windows.
  5. Registre su licencia. Consulte el apartado Windows: Registro de licencias.
  6. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
  7. Supervise el servidor. Consulte el apartado Windows: Supervisión del servidor.
- Windows: Creación del ID de usuario y de directorios para la instancia del servidor  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
  - Windows: Configuración del servidor de IBM Spectrum Protect  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
  - Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
  -  Sistemas operativos Windows Windows: Inicio de la instancia del servidor en sistemas Windows  
En un entorno de producción, el método preferido para iniciar el servidor es como un servicio Windows. En un entorno en el que va a reconfigurar, probar o completar tareas de mantenimiento, inicie el servidor en primer plano o utilice la modalidad de mantenimiento.
  - Windows: Detención del servidor  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
  - Windows: Registro de licencias  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
  - Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
  - Windows: Ejecución de varias instancias de servidor en un solo sistema  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
  - Windows: Supervisión del servidor  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## Windows: Creación del ID de usuario y de directorios para la instancia del servidor

---

Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.


## Antes de empezar

Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado Windows: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento

1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.

### Sistemas operativos Windows

 **Sistemas operativos Windows** Cree un ID de usuario que será el propietario de la instancia del servidor IBM Spectrum Protect . Un ID de usuario puede poseer varias instancias del servidor de IBM Spectrum Protect . Identifique la cuenta de usuario que poseerá la instancia del servidor.

Cuando el servidor se inicia como un servicio de Windows, esta cuenta es la única en la que iniciará sesión dicho servicio. La cuenta de usuario debe tener autoridad administrativa en el sistema. Una cuenta de usuario puede poseer más de una instancia de servidor.

Si tiene varios servidores en un sistema y desea ejecutar cada uno de ellos con una cuenta de usuario distinta, cree una nueva cuenta de usuario en este paso.

Cree el ID de usuario.

Restricción: El ID de usuario debe cumplir la siguiente regla:

El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos (\_). El ID de usuario debe tener 30 caracteres o menos y no puede empezar por *ibm*, *sql*, *sys* o un número. El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

- a. Utilice el siguiente mandato de sistema operativo para crear el ID de usuario:


```
net user user_ID */add
```

Se le pedirá que cree y verifique una contraseña para el nuevo ID de usuario.

- b. Emita los siguientes mandatos del sistema operativo para añadir un nuevo ID de usuario a los grupos Administradores:

```
net localgroup Administrators user_ID /add
net localgroup DB2ADMNS ID_usuario /add
```

2. Cree los directorios necesarios para el servidor.

 **Sistemas operativos Windows** Cree directorios vacíos para cada elemento de la tabla y asegúrese de que el nuevo ID de usuario que acaba de crear tiene permiso de lectura y escritura en los directorios. La base de datos, el registro de archivado y el registro activo deben residir en volúmenes físicos distintos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El <i>directorio de instancias</i> del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir d:\tsm\server1</code>	
Los directorios de bases de datos	<code>mkdir d:\tsm\db001</code> <code>mkdir e:\tsm\db002</code> <code>mkdir f:\tsm\db003</code> <code>mkdir g:\tsm\db004</code>	
Directorio de registro de activo	<code>mkdir h:\tsm\log</code>	
Directorio de registro de archivado	<code>mkdir i:\tsm\archlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir j:\tsm\logmirror</code>	

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir k:\tsm\archlogfailover</code>	


Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.

## Windows: Configuración del servidor de IBM Spectrum Protect

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

### Acerca de esta tarea

 **Sistemas operativos Windows** Consejo: La consola de gestión de IBM Spectrum Protect, que es un complemento de Microsoft Management Console (MMC), ya no se entrega con IBM Spectrum Protect. El método preferido para configurar el servidor consiste en utilizar el asistente de configuración. Puede utilizar el asistente para completar varias tareas de configuración de servidor. Sin embargo, no puede utilizar el asistente para ampliar el esquema de Active Directory para que los clientes puedan descubrir servidores automáticamente.

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:


- **Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **Windows: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

## Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración


El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.

### Antes de empezar


Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.

 **Sistemas operativos Windows**

### Acerca de esta tarea



 **Sistemas operativos Windows** Consejo: La consola de IBM Spectrum Protect, que es un complemento MMC, ya no se suministra con IBM Spectrum Protect. El método preferido para configurar la instancia de servidor es utilizar el asistente de configuración. Puede utilizar el asistente para completar varias tareas de configuración.

### Procedimiento

1. Asegúrese de que se cumplen los siguientes requisitos:  **Sistemas operativos Windows**
  - Asegúrese de que se cumplen los siguientes requisitos:
    - a. Pulse Inicio > Herramientas administrativas > Servicios.
    - b. En la ventana Servicios, seleccione el servicio Registro remoto si no está iniciado y, a continuación, pulse Iniciar.
  - Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:

- a. Pulse Inicio > Panel de control > Firewall de Windows.
- b. Seleccione Configuración avanzada.
- c. Seleccione Reglas de entrada en el panel izquierdo.
- d. Seleccione Nueva regla en el panel derecho.
- e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones de dominio y redes privadas.
- o Configure Control de cuenta de usuario:


Acceda a los tres valores de configuración de control de cuentas de usuario accediendo en primer lugar a las opciones de Seguridad de política de seguridad local, utilizando los pasos siguientes:

- a. Habilite la cuenta de Administrador incorporada:
    - Seleccione Cuentas: estado de la cuenta de administrador.
    - Seleccione Habilitar y pulse Aceptar.
  - b. Inhabilite el Control de cuentas de usuario para todos los administradores de Windows:
    - Seleccione el Control de cuentas de usuario: ejecutar todos los administradores en modalidad de aprobación de administrador.
    - Seleccione Inhabilitar y pulse Aceptar.
  - c. Inhabilite el Control de cuentas de usuario para la cuenta de Administrador incorporada:
    - Seleccione el Control de cuentas de usuario: modalidad de aprobación de administrador para la cuenta de Administrador incorporada.
    - Seleccione Inhabilitar y pulse Aceptar.
  - o Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
- o  Sistemas operativos Windows Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración. O, pulse dos veces en el programa `dsmi cfgx.exe` en `installation_directory\server`. El directorio predeterminado es `C:\Archivos de programa\Tivoli\TSM`.
- Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.
-  Sistemas operativos Windows Windows: Configuración de Remote Execution Protocol en Windows Configurar valores de acceso remoto utilizando estos procedimientos.

## Windows: Configuración de la instancia del servidor manualmente

---

Después de instalar IBM Spectrum Protect Versión 8.1.3, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

- Windows: Creación de una instancia del servidor  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.
-  Sistemas operativos Windows Windows: Configuración de comunicaciones de servidor y de cliente  
Tras instalar el servidor, puede configurar comunicaciones de cliente y servidor especificando opciones en los archivos de opciones de servidor y cliente.
- Windows: Formateo de la base de datos y las anotaciones  
Utilice el programa de utilidad `DSMSERV FORMAT` para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## Windows: Creación de una instancia del servidor


---

Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.

### Acerca de esta tarea

---

Puede tener una o más instancias del servidor en una estación de trabajo.

 Sistemas operativos Windows Importante: Antes de ejecutar el mandato `db2icrt`, asegúrese de que el usuario y el directorio de la instancia del usuario existen. Si no existe ningún directorio de instancia, debe crearlo.

El directorio de instancia almacena los siguientes archivos para la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`



- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

#### Sistemas operativos Windows

1. Inicie sesión como administrador y cree una instancia de IBM Spectrum Protect utilizando el mandato `db2icrt`. Especifique el siguiente mandato en una línea. La cuenta de usuario que especifique pasará a ser el ID de usuario que posea la Versión 8.1.3 o un servidor posterior (el ID de usuario de la instancia).

```
db2icrt -u cuenta_usuario nombre_instancia
```

Por ejemplo, si la cuenta de usuario es `tsminst1` y la instancia de servidor es `Server1`, debe especificar el siguiente mandato:

```
db2icrt -u tsminst1 server1
```

Se le pedirá la contraseña del ID de usuario `tsminst1`. Posteriormente, cuando crea y formatea la base de datos, utiliza el nombre de la instancia que especificó con este mandato con la opción `-k`.

2. Cambie la vía de acceso predeterminada para la base de datos para que sea la unidad en la que se encuentra el directorio de instancia del servidor. Realice los siguientes pasos:

- a. Haga clic en Inicio > Programas > IBM DB2 > DB2TSM1 > Command Line Tools > Command Line Processor.
- b. Escriba `abandonar` para salir del procesador de línea de mandatos.

Ahora debería abrirse una ventana con un indicador de mandatos, con el entorno correctamente configurado para emitir mandatos en los siguientes pasos.

- c. Desde el indicador de mandatos de esa ventana, emita el siguiente mandato para configurar la variable de entorno para la instancia de servidor con la que trabaja:

```
set db2instance=instance_name
```

Aquí `nombre_instancia` es el mismo nombre de instancia especificado al emitir el mandato `db2icrt`. Por ejemplo, para establecer la variable de entorno para la instancia del servidor `Server1`, emita el siguiente mandato:

```
set db2instance=server1
```

- d. Emita el mandato para configurar la unidad predeterminada:

```
db2 update dbm cfg using dftdbpath instance_location
```

Por ejemplo, el directorio de instancia es `d:\tsm\server1` y la ubicación de la instancia es la unidad `d:`. Escriba el mandato:

```
db2 update dbm cfg using dftdbpath d:
```

3. Cree un archivo de opciones de servidor. Consulte Windows: Configuración de comunicaciones de servidor y de cliente.

#### Sistemas operativos Windows

## Windows: Configuración de comunicaciones de servidor y de cliente

Tras instalar el servidor, puede configurar comunicaciones de cliente y servidor especificando opciones en los archivos de opciones de servidor y cliente.

### Acerca de esta tarea




Establezca estas opciones del servidor antes de iniciar el servidor. Cuando inicie el servidor, entrarán en vigor las nuevas opciones. Si modifica cualquiera de las opciones del servidor después de iniciarlo, debe detener el servidor y reiniciarlo para activar las opciones actualizadas.

Revise el archivo de opciones del servidor (`dsmserv.opt.smp`) que se encuentra en el directorio de instancias del servidor para ver y especificar las opciones de comunicaciones del servidor. De forma predeterminada, el servidor utiliza los métodos de comunicación TCP/IP y Named Pipes.

Consejo: Si al iniciar la consola del servidor ve mensajes de aviso que advierten de que el servidor no puede utilizar un protocolo, puede deberse a que el protocolo no esté instalado o a que la configuración no coincida con la del protocolo de Windows.

Para que un cliente utilice un protocolo activado en el servidor, el archivo de opciones del cliente debe contener los valores correspondientes para las opciones de comunicación. En el archivo de opciones del servidor, puede ver los valores de cada protocolo.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- Protocolo de control de transmisiones/protocolo Internet, versión 4 o versión 6
- Named Pipes
- Memoria compartida
- capa de sockets seguros (SSL)  
Consejo: Puede autenticar contraseña con el servidor de directorio LDAP o autenticar contraseñas con el servidor. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.
-  Sistemas operativos Windows: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos Windows: Establecimiento de opciones de Named Pipes  
El método de comunicación Named Pipes es idóneo cuando se ejecuta el servidor y el cliente en la misma máquina Windows. Named Pipes no necesita una configuración especial.
-  Sistemas operativos Windows: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## Windows: Establecimiento de opciones de TCP/IP

---

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea

---


Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.


```
commethod tcpip
tcpport 1500
tcpwindowsize 0
tcpnodelay yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPORT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.

 Sistemas operativos Windows: TCPWINDOWSIZE

 Sistemas operativos Windows: Especifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPORT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## Windows: Establecimiento de opciones de Named Pipes

---

El método de comunicación Named Pipes es idóneo cuando se ejecuta el servidor y el cliente en la misma máquina Windows. Named Pipes no necesita una configuración especial.

## Acerca de esta tarea

---

Éste es un ejemplo de configuración de Named Pipes:

```
commmethod namedpipe
 namedpipename \\.\pipe\adsmpipe
```

COMMETHOD se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:

```
commethod tcpip
commethod namedpipe
```

## Windows: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.


## Windows: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.

Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.

 **Sistemas operativos Windows** Importante: El programa de instalación crea un conjunto de claves de registro. Una de estas claves señala al directorio en el que se crea el servidor predeterminado, denominado SERVER1. Para instalar un servidor adicional, cree un directorio y utilice el programa de utilidad DSMSERV FORMAT con el parámetro -k, desde dicho directorio. Ese directorio se convierte en la ubicación del servidor. El registro realiza un seguimiento de los servidores instalados.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  **Sistemas operativos Windows**

```
db2set -i server1 DB2NOEXITLIST=ON
```

### Inicialización de una instancia del servidor


---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es */tsminst1*, emita los mandatos siguientes:  **Sistemas operativos Windows**

```
cd \tsminst1
dmserv -k server2 format dbdir=d:\tsm\db001 activeologsize=32768
activeologdirectory=e:\tsm\activeolog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

**Información relacionada:**

 DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)

## Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos

---


Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.


### Acerca de esta tarea

---

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos BACKUP DB o RESTORE DB.

Atención: Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 Sistemas operativos Windows Restricción: La copia de seguridad y restauración de base de datos sobre memoria compartida no está disponible en sistemas Windows.

 Sistemas operativos Windows En los siguientes mandatos, los ejemplos empleados son `server1` como instancia de la base de datos y `d:\tsmserv1` para el directorio del servidor de IBM Spectrum Protect. Sustituya estos valores por sus valores reales en los mandatos.

1. Cree un archivo que se llame `tsmdbmgr.env` en el directorio `d:\tsmserv1` con el siguiente contenido:

```
DSMI_CONFIG=directorio_instancia_servidor\tsmdbmgr.opt
DSMI_LOG=directorio_instancia_servidor
```

2. Establezca la configuración de la variable de entorno `DSMI_api` para la instancia de la base de datos:

- a. Abra una ventana de mandatos de DB2. Uno de los métodos consiste en ir al directorio `C:\Archivo de programas\Tivoli\TSM\db2\bin`, o si ha instalado IBM Spectrum Protect en una ubicación diferente, ir al subdirectorio `db2\bin` de su directorio de instalación principal. Después, emita este mandato:

```
db2cmd
```

- b. Emita este mandato:

```
db2set -i server1 DB2_VENDOR_INI=d:\tsmserv1\tsmdbmgr.env
```

3. Cree un archivo que se denomine `tsmdbmgr.opt` en el directorio `d:\tsmserv1` con el siguiente contenido:

```

nodename $$_TSMDBMGR_$$
commethod tcpip
tcpserveraddr localhost
tcpport 1500
passwordaccess generate
errorlogname d:\tsmserv1\tsmdbmgr.log
```

donde

- o `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Este valor debe ser `$_TSMDBMGR_$$` para que una copia de seguridad de base de datos funcione.
- o `commethod` especifica la API de cliente utilizada para ponerse en contacto con el servidor para la copia de seguridad de base de datos.
- o `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
- o `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmserv.opt`.
- o se requiere `passwordaccess` para que el nodo de copia de seguridad se conecte al servidor en el sistema Windows.
- o `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin

embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.

## Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor


---

Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

### Acerca de esta tarea

---

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.


 Sistemas operativos Windows Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.

Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

### Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos Windows Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancias del servidor mediante el editor de texto. Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `c:\Program Files\Tivoli\TSM`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.

- a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```

4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.


#### Información relacionada:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 Sistemas operativos Windows

## Windows: Inicio de la instancia del servidor en sistemas Windows

En un entorno de producción, el método preferido para iniciar el servidor es como un servicio Windows. En un entorno en el que va a reconfigurar, probar o completar tareas de mantenimiento, inicie el servidor en primer plano o utilice la modalidad de mantenimiento.

### Antes de empezar

Seleccione uno de los siguientes métodos para iniciar el servidor:

Como un servicio de Windows

Este método resulta útil en un entorno de producción. Cuando configure el servidor para que se ejecute como un servicio, puede especificar que el servidor se inicie automáticamente siempre que se inicie el sistema.

En el primer plano

Este método es útil cuando está configurando o probando el servidor. Cuando inicia el servidor en segundo plano, IBM Spectrum Protect proporciona un ID de usuario de administrador especial que se denomina SERVER\_CONSOLE. Todos los mensajes de servidor se muestran en primer plano. Los mensajes pueden ser útiles si debe depurar problemas de inicio.


En modalidad de mantenimiento

Este método resulta útil cuando va a completar tareas de mantenimiento o reconfiguración. Cuando inicie el servidor en modalidad de mantenimiento, debe inhabilitar las operaciones que puedan interrumpir las tareas de mantenimiento o reconfiguración.

### Procedimiento

Siga las instrucciones para la opción seleccionada:

Opción	Descripción
<b>Inicio del servidor como un servicio de Windows.</b>	Para iniciar el servidor como un servicio de Windows, lleve a cabo una de las siguientes acciones: <ul style="list-style-type: none"><li>• Si ha configurado el servidor utilizando el asistente de configuración, realice los siguientes pasos:<ol style="list-style-type: none"><li>a. Configure el servidor para que se inicie como un servicio de Windows siguiendo las instrucciones de Windows: Configuración del servidor para que se inicie como un servicio de Windows.</li><li>b. Inicie el servidor siguiendo las instrucciones de Windows: Inicio del servidor como un servicio de Windows..</li></ol></li><li>• Si no ha utilizado el asistente de configuración cree y configure el servicio Windows siguiendo las instrucciones de Windows: Creación manual y configuración de un servicio de Windows.</li></ul>
<b>Inicio del servidor en segundo plano</b>	Para iniciar el servidor en segundo plano, siga las instrucciones en Windows: Inicio del servidor en segundo plano.
<b>Inicio del servidor en modalidad de mantenimiento</b>	Para iniciar el servidor en modalidad de mantenimiento, siga las instrucciones de Windows: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos Windows

## Windows: Configuración del servidor para que se inicie como un servicio de Windows

Antes de poder iniciar el servidor como un servicio de Windows, debe asegurarse de que las opciones y los derechos de acceso se han establecido correctamente.

### Antes de empezar

Se debe crear un servicio de Windows. Si ha configurado el servidor utilizando el asistente de configuración, se ha creado automáticamente un servicio Windows. En ese caso, utilice este procedimiento para configurar el servidor para que se inicie como un servicio de Windows.

Si no ha utilizado un asistente, debe crear y configurar el servicio de Windows de forma manual siguiendo los pasos de Windows: Creación manual y configuración de un servicio de Windows.

### Procedimiento

1. Desde el menú de Windows Inicio, pulse Ejecutar, escriba `services.msc`, y pulse Aceptar.
2. En la ventana Servicios, seleccione la instancia del servidor que desea iniciar como servicio, y pulse Propiedades. Por ejemplo, seleccione TSM INST1, y pulse Propiedades.
3. Para asegurarse de que el servicio del servidor inicia automáticamente, pulse la pestaña General. Desde la lista Tipo de inicio, seleccione Automático.
4. Para establecer el usuario para que inicie el servicio de servidor, pulse el separador Iniciar sesión y realice una de las acciones siguientes:
  - o Si tiene previsto ejecutar el servicio de servidor bajo la cuenta de sistema local, seleccione Cuenta de sistema local y pulse Aceptar.
  - o Si piensa ejecutar el servicio de servidor bajo el ID de usuario de instancia, realice las acciones siguientes:
    - a. Seleccione Esta cuenta, y navegue hasta el ID de usuario propietario de la instancia DB2 del servidor y que tiene permisos para iniciar el servidor.
    - b. En la ventana Seleccionar usuario, en el campo Escriba el nombre de objeto a seleccionar, escriba el ID de usuario.
    - c. Pulse Comprobar nombres.
    - d. Pulse Aceptar dos veces.
5. Si ha configurado el servicio de servidor para que se ejecute bajo la cuenta de sistema local, otorgue acceso de base de datos a la cuenta de sistema local:
  - a. Inicie sesión con el ID de usuario que se utilizó para crear la base de datos de servidor. Este ID de usuario es el ID de usuario que se utiliza para ejecutar el programa de utilidad DSMSERV FORMAT para inicializar la base de datos de servidor. De forma alternativa, si ha configurado el servidor con el asistente de configuración `dsmicfgx`, este ID de usuario es el ID de usuario que se ha utilizado para crear la instancia.
  - b. Abra una ventana de mandatos de DB2. Si el servidor está instalado en Windows Server 2012, abra la ventana Inicio y pulse Ventana de mandatos DB2 - Administrador.
  - c. En la ventana de mandatos de DB2, especifique los siguientes mandatos:

```
set DB2INSTANCE=server1
db2 connect to TSMDB1
db2 grant dbadm with dataaccess with accessctrl on database to user system
db2 grant secadm on database to user system
```

Consejo: Si se configura el servicio del servidor para que se ejecute bajo la cuenta del Sistema local, cualquier administrador del sistema puede acceder a la base de datos. Además, cualquier administrador que pueda iniciar sesión en el sistema puede ejecutar el servidor.

## Qué hacer a continuación

---

Para iniciar el servicio, siga las instrucciones en Windows: Inicio del servidor como un servicio de Windows..

 Sistemas operativos Windows

## Windows: Inicio del servidor como un servicio de Windows.

---

Si está ejecutando el sistema operativo IBM Spectrum Protect on a Windows, puede iniciar el servidor como un servicio.

## Antes de empezar

---

Se debe crear un servicio de Windows. El servicio se ha creado automáticamente si ha configurado el servidor utilizando el asistente de configuración.. Si el servicio se ha creado automáticamente, debe configurar el servidor para que se inicie como un servicio siguiendo los pasos en Windows: Configuración del servidor para que se inicie como un servicio de Windows. A continuación, utilice este procedimiento para iniciar el servidor como un servicio.

Si no ha utilizado el asistente de configuración para crear el servicio, debe crear y configurar el servicio manualmente. Siga los pasos descritos en Windows: Creación manual y configuración de un servicio de Windows.

## Procedimiento

---

Para iniciar el servidor como un servicio de Windows, siga estos pasos:


1. Inicie sesión en el servidor con un ID de usuario que está en el grupo de administradores.
2. Desde el menú de Windows Inicio, pulse Ejecutar, escriba `services.msc`, y pulse Aceptar.
3. En la ventana Servicios, seleccione la instancia del servidor que desea iniciar, y pulse Iniciar.

## Qué hacer a continuación

---

Debido que el servicio del servidor puede emitir solicitudes que requieren tomar una acción, es importante supervisar la actividad del servidor con el Centro de operaciones o el cliente administrativo.

Para ver los mensajes de inicio y detención registrados en el registro de aplicaciones de Windows, use la herramienta Visor de sucesos en la carpeta Herramientas administrativas.

 Sistemas operativos Windows

## Windows: Creación manual y configuración de un servicio de Windows

---

Si ha configurado el servidor utilizando el asistente de configuración, se ha creado automáticamente un servicio Windows. Si no se ha creado un servicio automáticamente, debe crearlo.

### Antes de empezar

---

Para completar este procedimiento, debe iniciar la sesión con un ID de usuario que esté en el grupo de administradores.

### Procedimiento

---

Para crear un servicio de Windows y configurar las opciones de inicio del servicio, complete el paso siguiente:

Abra una ventana de mandatos y entre el mandato `sc.exe create`:

```
sc.exe create nombre_servidor binPath= "vía_acceso_a_servidor -k nombre_instancia"
start= tipo_inicio obj= nombre_cuenta password= contraseña
```

donde:

*nombre\_servidor*

Especifica el nombre del servicio de servidor.

*vía\_acceso\_a\_servidor*

Especifica la vía de acceso al archivo ejecutable `dedsmvc.exe`, incluyendo el nombre de archivo. Esta vía de acceso es la vía de acceso predeterminada:

`C:\Archivos de programa\Tivoli\TSM\server`

*nombre\_instancia*

Especifica el nombre de la instancia de DB2, que también es el nombre de la instancia de servidor, por ejemplo `Server1`.

*tipo\_inicio*

Especifica el método para iniciar el servicio. Para iniciar automáticamente el servicio, entre `auto`. Si especifica la opción `auto`, el servicio se inicia automáticamente al arrancar el sistema y se reinicia automáticamente siempre que se reinicia el sistema. Para iniciar manualmente el servicio, entre `demand`.

*nombre\_cuenta*

Especifica el ID de usuario de la cuenta bajo la que se ejecuta el servicio. Por ejemplo, el nombre de cuenta puede ser `Administrator`. Este parámetro es opcional. Si no se especifica, se utiliza la cuenta del sistema local.

*contraseña*


Especifica la contraseña para la cuenta de usuario de *nombre\_cuenta*.

Consejo: Cuando entre el mandato, asegúrese de entrar un espacio después de cada signo de igual (=).

### Resultados

---

El servidor se inicia como un servicio Windows.

 Sistemas operativos Windows

## Windows: Inicio del servidor en segundo plano

---

Para interactuar de forma directa con un servidor de IBM Spectrum Protect, inicie el servidor en segundo plano. Por ejemplo, si desea escribir mandatos, inicie el servidor en segundo plano.

### Procedimiento

---

1. Cambie al directorio donde está instalado el servidor. Por ejemplo, cambie el directorio `c:\Archivos de programa\tivoli\tsm\server`.
2. Entre el mandato siguiente:

```
dsmserv -k nombre_instancia
```



donde *nombre\_instancia* especifica la instancia de servidor.



## Windows: Servicios asociados al servidor en sistemas Windows

Cuando se inicia el servidor IBM Spectrum Protect como un servicio, otros servicios se inician automáticamente. Estos servicios están asociados con el gestor de la base de datos, DB2.

Los servicios siguientes están asociados al servidor.

Nombre del servicio	Finalidad	Comentarios.
TSM <i>Server_instan ce</i>	El servicio para la instancia de servidor que se llama <i>instancia_servidor</i> .  Por ejemplo: TSM <i>Server1</i>	Defina las opciones de inicio y parada de este servicio para que inicien y detengan la instancia del servidor automáticamente.  Cada instancia del servidor se ejecuta como un servicio diferente.
DB2 - DB2TSM1 - <i>SERVER_INSTAN CE</i>	El servicio de DB2 para la instancia del servidor se llama <i>Server_instance</i> .  Por ejemplo: DB2 - DB2TSM1 - <i>SERVER1</i>	Este servicio se inicia automáticamente cuando se inicia el servicio para la instancia de servidor. El servicio DB2 no se detiene de forma automática cuando detiene el servicio del servidor.  El sistema tiene uno de estos servicios para cada servicio de la instancia del servidor que se inicia en el sistema.
DB2 Governor (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 License Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 Management Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 Remote Command Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.



## Windows: Inicio del servidor en modalidad de mantenimiento

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

### Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSEV con el parámetro MAINTENANCE.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, *dmserv.opt*, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

## Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

## Qué hacer a continuación

---

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## Windows: Detención del servidor

---

Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

### Acerca de esta tarea

---

Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:

```
halt
```

## Windows: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

### Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

### Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

### Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

### Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

## Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

## Ejemplo

---

Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:


```
set dbrecovery dbback
```

## Windows: Ejecución de varias instancias de servidor en un solo sistema

---

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.


Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.


 **Sistemas operativos Windows** El conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos detallados en Windows: Creación de una instancia del servidor para cada instancia nueva, de forma opcional creando el usuario de instancia nuevo.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.


Puede actualizar directamente de V7.1 a V8.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.3 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

 **Sistemas operativos Windows** Una instalación típica de IBM Spectrum Protect incluye una instancia del servidor en el sistema servidor de IBM Spectrum Protect. Es posible que desee instalar una segunda instancia si está configurando un entorno en clúster. También puede que desee ejecutar más de un servidor en un sistema grande si tiene varias bibliotecas de cintas o una configuración sólo de disco. Después de instalar y configurar el primer servidor de IBM Spectrum Protect, utilice el asistente de inicialización del servidor para crear instancias adicionales del servidor de IBM Spectrum Protect en el mismo sistema.

 **Sistemas operativos Windows** mediante el asistente de inicialización del servidor puede instalar hasta cuatro instancias del servidor de IBM Spectrum Protect en un solo sistema o clúster.

### Tareas relacionadas:

 Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## Windows: Supervisión del servidor

---

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## Procedimiento

---

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de espacio de las anotaciones activas, pero durante poco tiempo.
  - Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.
- Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tarden más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

#### 2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible.

Recuerde: Si el registro de archivado y el registro de archivado de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.

Probablemente observará el siguiente patrón:

- a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
- b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.
- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## Windows: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al

último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.3 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.3, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado Windows: Revertir de la versión 8.1.3 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:


```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
8.  Sistemas operativos Windows Cambie al directorio en el que colocó el archivo ejecutable. A continuación, pulse dos veces en el siguiente archivo ejecutable o introduzca el siguiente mandato en la línea de mandatos para extraer los archivos de instalación.

Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.

`8.x.x.x-IBM-SPSRV-plataforma.exe`

donde: *plataforma* indica el sistema operativo en el que se va a instalar IBM Spectrum Protect.

9. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.

Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.

Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

Asistente de instalación

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect en modalidad de consola

Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.

## Resultados

---

Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos WindowsC:\ProgramData\IBM\Installation Manager\logs
-  Sistemas operativos WindowsWindows: Aplicación de un fixpack a IBM Spectrum Protect 8.1.3 en un entorno en clúster para Windows  
Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.3.

## Windows: Revierta de la versión 8.1.3 a un servidor anterior

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

## Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:


- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

## Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.3 al 8.1.2 o del 8.1.3 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.

-  **Sistemas operativos Windows**: Reversión a la versión de servidor anterior en una configuración de clúster  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.


## Pasos para recuperar la versión anterior del servidor


---

### Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

### Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato:  
 **Sistemas operativos Windows**  

```
dmserv -k nombre_instancia removedb tsmdb1
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado Windows: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.3. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato:  **Sistemas operativos Windows**  

```
/dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.
7. Restaure la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - o Archivo de configuración de dispositivos
  - o Archivo histórico de volúmenes
  - o El archivo de opciones de servidor (generalmente dmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.3, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de seguridad de la base de datos. Utilice el mandato RESTORE VOLUME.  
Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:  

```
audit volume nombre_volumen fix=yes
```
11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

---

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.3, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.3.

### Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.3:

- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.3. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

### Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:
  - Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.3.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro REUSEDELAY para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.3. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.3, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.3.

## Windows: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect

---

Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.

### Finalidad





---

Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.




Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.



Tabla 1. Mandatos de DB2

Mandato	Descripción	Ejemplo
 Sistemas operativos Windows Windows db2cmd	 Sistemas operativos Windows Abre la ventana del procesador de línea de mandatos de DB2 e inicializa el entorno de línea de mandatos de DB2.	 Sistemas operativos Windows Abra la ventana de mandatos de DB2:  db2cmd
db2icrt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia. Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p>  Sistemas operativos Windows Este programa de utilidad se encuentra en el directorio DB2PATH\bin, donde DB2PATH es la ubicación en la que se instala la copia de DB2.	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre> /opt/tivoli/tsm/db2/instance / db2icrt -a server -u nombre_instancia nombre_instancia         </pre>
db2set	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> db2set
CATALOG DATABASE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	<p>Catalogue la base de datos:</p> db2 catalog database tsmdb1
CONNECT TO DATABASE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	<p>Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:</p> db2 connect to tsmdb1

Mandato	Descripción	Ejemplo
GET DATA BASE CON FIGU RATI ON	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Muestre la información de configuración para un alias de base de datos:  db2 get db cfg for tsmdb1  Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.  db2 get db config for tsmdb1 show detail
GET DATA BASE MAN AGER CON FIGU RATI ON	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEAL TH SNAP SHOT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsmdb1
GRA NT (Auto rizaci ones de base de datos )	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser

Man dato	Descripción	Ejemplo
RUNSTATS	<p>Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.</p> <p>Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.</p> <p>Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.</p> <p>Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.</p>	<p>Actualice las estadísticas en una única tabla.</p> <pre>db2 runstats on table SCHEMA_NAME.TA BLE_NAME with distribution and sampled detailed indexes all</pre>
 Sistemas operativos Windows	<p> Sistemas operativos Windows</p> <p>Determina qué instancia se aplica a la sesión actual.</p>	<p> Sistemas operativos Windows</p> <p>Determine qué instancia es aplicable:</p> <pre>set db2instance=ts minst1</pre>
SETSCHEMA	<p>Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2.</p> <p>Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.</p>	<p>Establezca el esquema para IBM Spectrum Protect:</p> <pre>db2 set schema tsmdb1</pre>
START DATABASE MANAGER	<p>Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Inicie el gestor de base de datos:</p> <pre>db2start</pre>
STOP DATABASE MANAGER	<p>Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.</p> <p>Este mandato no es válido en un cliente.</p> <p>El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Detenga el gestor de base de datos:</p> <pre>db2 stop dbm</pre>

## Windows: Desinstalar IBM Spectrum Protect


Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.

- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

 Sistemas operativos Windows Atención: No utilice la herramienta Agregar/Eliminar programas en el panel de control de Windows para desinstalar IBM Spectrum Protect. Use solamente el procedimiento de desinstalación que se describe en esta sección.

## Acerca de esta tarea

---

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.
- Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- Windows: Desinstalación e instalación de IBM Spectrum Protect  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- Windows: Desinstalación de IBM Installation Manager  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

## Qué hacer a continuación

---

Consulte Windows: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico

---

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento

---

1. Inicie el Installation Manager.

 Sistemas operativos Windows Abra el Installation Manager desde el menú de Inicio.

2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.


## Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola

---


Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.


### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Windows eclipse\tools

Por ejemplo:

-  Sistemas operativos Windows C:\Archivos de programa\IBM\Installation Manager\eclipse\tools

2. Desde el directorio herramientas, emita el siguiente mandato:
  -  Sistemas operativos Windows `imcl.exe -c`
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique N para Siguiente.
6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
7. Especifique N para Siguiente.
8. Escriba U para Desinstalar.
9. Escriba F para Finalizar.

## Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.


### Antes de empezar

Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.


Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.

Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


### Procedimiento

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Windows `eclipse\tools`

Por ejemplo:

-  Sistemas operativos Windows `C:\Archivos de programa\IBM\Installation Manager\eclipse\tools`

2. Desde el directorio herramientas, emita el siguiente mandato, donde `archivo_respuestas` representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

 Sistemas operativos Windows

```
imcl.exe -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos Windows


```
imcl.exe -input C:\tmp\input\uninstall_response.xml -silent
```

## Windows: Desinstalación e instalación de IBM Spectrum Protect

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.


### Acerca de esta tarea

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos Windows Realice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:

```
db2ilist
```


2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:

 Sistemas operativos Windows

```
db2 attach to server1
db2 get dbm cfg show detail
db2 detach
```


Mantenga un registro de la ruta de base de datos para casa instancia.

3. Desinstale IBM Spectrum Protect. Consulte el apartado Windows: Desinstalar IBM Spectrum Protect.

 Sistemas operativos Windows Tras desinstalar IBM Spectrum Protect, compruebe en el Panel de control > Añadir o quitar programas con el fin de verificar que la base de datos IBM Spectrum Protect DB2 está desinstalada.

4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten los credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estos credenciales utilizando la variable `INSTANCE_CRED`.

Puede encontrar el archivo de instancias en la siguiente ubicación:

- o  Sistemas operativos Windows `C:\ProgramData\IBM\Tivoli\TSM\instanceList.obj` en el directorio de instalación del servidor de IBM Spectrum Protect

5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado Windows: Instalación de los componentes de servidor.

Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- a. Vuelva a crear las instancias de servidor. Consulte el apartado Windows: Creación de una instancia del servidor. Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- b. Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos Windows

```
set db2instance=server1
db2 catalog database tsmdb1
db2 attach to server1
db2 update dbm cfg using dftdbpath instance_drive
db2 detach
```

- c. Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```

Si figura TSMDDB1 puede iniciar el servidor.

## Windows: Desinstalación de IBM Installation Manager


---

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

### Antes de empezar

---

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.

 Sistemas operativos Windows Para ver los paquetes instalados, pulse Inicio > Todos los programas > IBM Installation Manager > Ver paquetes instalados.

### Procedimiento

---

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos Windows

1. En el menú Inicio, pulse Panel de control > Programas y características.
2. Seleccione IBM Installation Manager y pulse Desinstalar.

## Actualización a V8.1







---

Para sacar partido de las nuevas características del producto y de las actualizaciones, actualice el servidor IBM Spectrum Protect a la versión 8.1.3.

## Acerca de esta tarea

Para actualizar el servidor en el mismo sistema operativo, consulte las instrucciones de actualización. Para ver las instrucciones sobre la migración del servidor a un sistema operativo distinto, consulte IBM Spectrum Protect Proceso de migración y actualización: preguntas más frecuentes.

Tabla 1. Instrucciones de actualización

Para actualizar desde esta versión	A esta versión	Consulte esta información
V8.1	Fixpack o arreglo temporal V8.1	 Sistemas operativos AIX Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Linux Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Windows Instalación de un fixpack de servidor de IBM Spectrum Protect
V7.1	V8.1	Instalación del servidor y comprobación de la actualización
V7.1	Fixpack o arreglo temporal V8.1	 Sistemas operativos AIX Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Linux Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Windows Instalación de un fixpack de servidor de IBM Spectrum Protect
V5.5, V6.2 o V6.3	V8.1	IBM Spectrum Protect Proceso de actualización y migración: preguntas más frecuentes

Una actualización de la versión 7 a la 8.1 ocupa entre 20 y 50 minutos. El entorno puede generar resultados distintos que los obtenidos en los laboratorios.

Para obtener información acerca de las actualizaciones en un entorno en clúster, consulte Actualización del servidor en un entorno en clúster.

Para volver a una versión anterior del servidor después de una actualización o migración, debe tener una copia de seguridad de la base de datos completa y el software de instalación para el servidor original. También debe tener archivos de configuración claves siguientes:

- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor
- Actualización a V8.1  
Puede actualizar el servidor directamente de la versión 7.1 a la 8.1. No tiene que desinstalar la versión 7.1.
- Actualización del servidor en un entorno en clúster  
Para actualizar un servidor a V8.1.3 en un entorno en clúster, debe completar las tareas de preparación e instalación. Los procedimientos varían, dependiendo del sistema operativo y el release.

### Información relacionada:

 [IBM Spectrum Protect Proceso de migración y actualización: preguntas más frecuentes](#)

## Actualización a V8.1

Puede actualizar el servidor directamente de la versión 7.1 a la 8.1. No tiene que desinstalar la versión 7.1.

### Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor que se va a actualizar. Si ha instalado los componentes de servidor desde un DVD, asegúrese de que el DVD está disponible. Si ha instalado los componentes del servidor desde un paquete descargado, asegúrese de que los archivos descargados están disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Consejo: A partir de la versión 8.1, dejará de haber DVD disponibles.

## Procedimiento

---

Para actualizar el servidor a V8.1, realice estas tareas:

- **Planificación de la actualización**  
Antes de actualizar el servidor de V7.1 a V8.1, debe revisar la información de planificación más importante, como los requisitos del sistema y las notas del release. A continuación, seleccione el día y la hora correspondiente para actualizar el sistema de manera que pueda minimizar el impacto sobre las operaciones de producción.
- **Preparación del sistema**  
Para preparar el sistema para la actualización de V7.1 a V8.1, tiene que recopilar información sobre cada instancia de DB2. Luego, realice una copia de seguridad de la base de datos del servidor, guarde los archivos de configuración, cancele las sesiones y detenga el servidor.
- **Instalación del servidor y comprobación de la actualización**  
Para completar el proceso de actualización del servidor a V8.1, tiene que instalar el servidor V8.1. A continuación, compruebe que la actualización haya sido satisfactoria al iniciar la instancia del servidor.

## Planificación de la actualización

---

Antes de actualizar el servidor de V7.1 a V8.1, debe revisar la información de planificación más importante, como los requisitos del sistema y las notas del release. A continuación, seleccione el día y la hora correspondiente para actualizar el sistema de manera que pueda minimizar el impacto sobre las operaciones de producción.

### Acerca de esta tarea


---

En las pruebas de laboratorio, el proceso de actualización del servidor de V7.1 a V8.1 ocupó entre 14 y 45 minutos. Los resultados que obtiene pueden variar, dependiendo del entorno de hardware y de software y el tamaño de la base de datos del servidor.


## Procedimiento

---

1. Revise los requisitos de hardware y software:

 Sistemas operativos AIX Requisitos del sistema para los sistemas AIX

 Sistemas operativos Linux Requisitos del sistema para los sistemas Linux

 Sistemas operativos Windows Requisitos del sistema para los sistemas Windows

Para ver las últimas actualizaciones relacionadas con los requisitos del sistema, consulte el sitio web de soporte de IBM Spectrum Protect, nota técnica 1243309.

2. Para obtener instrucciones especiales o información específica para su sistema operativo, revise las Notas del release de los componentes del servidor de la Versión 8.1 y IBM Spectrum Protect los archivos readme del fixpack Versión 8.1.
3. Seleccione la fecha y la hora adecuadas para actualizar el sistema para minimizar el impacto en las operaciones de producción. La cantidad de tiempo necesaria para actualizar el sistema depende del tamaño de la base de datos y varios otros factores. Al iniciar el proceso de actualización, los clientes no pueden conectarse al servidor hasta que el nuevo software esté instalado y todas las licencias necesarias se registren de nuevo.
4. Si está actualizando el servidor de V6 o V7 a V8.1, verifique que dispone del ID de sistema y de la contraseña para la instancia de DB2 del servidor IBM Spectrum Protect. Estas credenciales son necesarias para actualizar el sistema.

## Preparación del sistema

---


Para preparar el sistema para la actualización de V7.1 a V8.1, tiene que recopilar información sobre cada instancia de DB2. Luego, realice una copia de seguridad de la base de datos del servidor, guarde los archivos de configuración, cancele las sesiones y detenga el servidor.

## Procedimiento

---

1. Inicie la sesión en el sistema donde se haya instalado el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux Asegúrese de haber iniciado sesión con el ID del usuario de la instancia.

 Sistemas operativos Windows Asegúrese de haber iniciado sesión con el ID del usuario administrativo que se usó para instalar el servidor V7.1.



2. Obtenga una lista de instancias DB2. Emita el siguiente mandato del sistema:

```
Systemas operativos AIX Systemas operativos Linux
/opt/tivoli/tsm/db2/instance/db2ilist
```

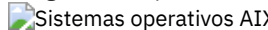
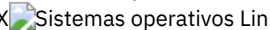
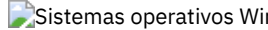
```
Systemas operativos Windows
db2ilist
```

La información podría ser similar al siguiente ejemplo:

```
Systemas operativos AIX Systemas operativos Linux
tsminst1
```

```
Systemas operativos Windows
SERVER1
```

Asegúrese de que cada instancia corresponde a un servidor que se está ejecutando en el sistema.

3.   Para cada instancia de DB2, tenga en cuenta la vía de acceso predeterminada de la base de datos, la vía de acceso real de la base de datos, el nombre de la base de datos, el alias de la base de datos y cualquier variable de DB2 que esté configurada para la instancia. Conserve el registro para referencias futuras. Esta información es obligatoria para restaurar la base de datos V7.1.
4.  Reúna la información acerca de cada instancia de DB2. Tenga en cuenta la vía de acceso a la base de datos predeterminada, la vía de acceso a la base de datos real, el nombre de la base de datos, el alias de la base de datos y cualquier variable de DB2 que esté configurada para la instancia. Conserve el registro para referencias futuras. Esta información es obligatoria para restaurar la base de datos V7.1.
  - a. Abra la ventana de mandatos de DB2 emitiendo el siguiente mandato del sistema:

```
db2cmd
```

b. Para cambiar la instancia, emita el siguiente mandato del sistema:

```
set DB2INSTANCE=instance
```

en donde *instancia* especifica la instancia de DB2.

c. Obtenga la vía de acceso predeterminada de la base de datos para la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2 get dbm cfg | findstr DFTDBPATH
```

La información podría ser similar al siguiente ejemplo:

```
Vía acceso base datos predeterminada (DFTDBPATH) = D:
```

d. Obtenga información acerca de las bases de datos de la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2 list database directory
```

La información podría ser similar al siguiente ejemplo:

```
Directorio de bases de datos del sistema
```

```
Número de entradas del directorio = 2
```

```
Entrada 1 de base de datos:
```

```
Alias de la base de datos = TSMAL001
Nombre de la base de datos = TSMDB1
Nombre del nodo = TSMNODE1
Nivel de release de la base de datos = d.00
Comentario = TSM SERVER DATABASE VIA TCPIP
Tipo de entrada de directorio = Remote
Número de partición de base de datos de catálogo = -1
Nombre host del servidor alternativo =
Número de puerto del servidor alternativo =
```

```
Entrada 2 de base de datos:
```

```
Alias de la base de datos = TSMDB1
Nombre de la base de datos = TSMDB1
Directorio local de la base de datos = D:
Nivel de release de la base de datos = d.00
```

```
Comentario =
Tipo de entrada de directorio = Indirect
Número partición base datos catálogo = 0
Nombre host del servidor alternativo =
Número de puerto del servidor alternativo =
```

e. Obtenga las variables de la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2set -all
```

La información podría ser similar al siguiente ejemplo:

```
[e] DB2CODEPAGE=1208
[e] DB2PATH=D:\TSM\db2
[i] DB2_PMODEL_SETTINGS=MAX_BACKGROUND_SYSAPPS:500
[i] DB2_SKIPINSERTED=ON
[i] DB2_KEEPTABLELOCK=OFF
[i] DB2_EVALUNCOMMITTED=ON
[i] DB2_VENDOR_INI=D:\Server1\tsmdbmgr.env
[i] DB2_SKIPDELETED=ON
[i] DB2INSTPROF=C:\ProgramData\IBM\DB2\DB2TSM1
[i] DB2COMM=TCPIP
[i] DB2CODEPAGE=819
[i] DB2_PARALLEL_IO=*
[g] DB2_EXTSECURITY=YES
[g] DB2_COMMON_APP_DATA_PATH=C:\ProgramData

[g] DB2PATH=D:\TSM\db2
[g] DB2INSTDEF=SERVER1
```

5. Conéctese al servidor utilizando un ID de usuario de administración.
6. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es crear una copia de seguridad de instantánea, que es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de base de datos planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea emitiendo el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

7. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio emitiendo el siguiente mandato de administración:

```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo. Consejo: Si decide restaurar la base de datos V7.1, se requiere este archivo.

8. Realice una copia de seguridad del archivo del historial del volumen a otro directorio. Emita el siguiente mandato de administración:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes. Consejo: Si decide restaurar la base de datos V7.1, se requiere este archivo.

9. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
10. Evite que haya actividad en el servidor inhabilitando nuevas sesiones. Emita los siguientes mandatos de administración:

```
disable sessions client
disable sessions server
```

11. Verifique si existen sesiones en curso y notifique a los usuarios que el servidor va a detenerse. Para comprobar las sesiones existentes, emita el siguiente mandato de administración:

```
query session
```

12. Cancele las sesiones emitiendo el siguiente mandato de administración:



```
cancel session all
```

Este mandato cancela todas las sesiones excepto la sesión actual.


13. Detenga el servidor emitiendo el siguiente mandato de administración:

```
halt
```

14. Verifique que el servidor está apagado y no hay ningún proceso en ejecución.

 Sistemas operativos AIX  Sistemas operativos Linux Emita el mandato siguiente:

```
ps -ef | grep dsmserv
```

 Sistemas operativos Windows Abra la aplicación del gestor de tareas de Windows y revise la lista de los procesos activos.

15. En el directorio de la instancia del servidor de la instalación, localice el archivo NODELOCK y trasládalo a otro directorio, donde va a guardar los archivos de configuración. El archivo NODELOCK contiene la información de las licencias anteriores de la instalación. Esta información de licencia se sustituye cuando finaliza la actualización.

**Referencia relacionada:**

BACKUP DB (copia de seguridad de la base de datos)  
BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)  
BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)  
DISABLE SESSIONS (Impedir que nuevas sesiones accedan a Tivoli Storage Manager)  
QUERY SESSION (Consultar sesiones de cliente)  
CANCEL SESSION (Cancelar una o más sesiones cliente)  
HALT (Concluir el servidor)



## Instalación del servidor y comprobación de la actualización


---

Para completar el proceso de actualización del servidor a V8.1, tiene que instalar el servidor V8.1. A continuación, compruebe que la actualización haya sido satisfactoria al iniciar la instancia del servidor.



### Antes de empezar

---

 Sistemas operativos AIX  Sistemas operativos Linux Debe haber iniciado sesión en el sistema haciendo uso del ID del usuario root.

 Sistemas operativos Windows Debe haber iniciado sesión en el sistema con el ID de usuario de administración que se utilizó para instalar el servidor anterior.

Puede obtener el paquete de instalación desde un sitio de descarga de IBM®.

 Sistemas operativos AIX  Sistemas operativos Linux Establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente.

1. Para consultar el valor de tamaño máximo de archivo, ejecute el mandato siguiente:

```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado completando las instrucciones de la documentación de su sistema operativo.

### Acerca de esta tarea

---

Haciendo uso del software de instalación de IBM Spectrum Protect, puede instalar los siguientes componentes:

- Servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- Idiomas de servidor
- Licencia
- Dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de los siguientes sitios web:
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información más reciente, actualizaciones y arreglos de mantenimiento, vaya al sitio de soporte de Tivoli Storage Manager: IBM Support Portal.
2. Realice los siguientes pasos:

 Sistemas operativos AIX  Sistemas operativos Linux

 Sistemas operativos AIX  Sistemas operativos Linux

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio, consulte el documento descargado de su

producto.

- IBM Spectrum Protect nota técnica 4042944
- IBM Spectrum Protect Extended Edition nota técnica 4042945
- IBM Spectrum Protect for Data Retention nota técnica 4042946


b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.

También, asegúrese de tener la autorización ejecutable del archivo del paquete.

c. En caso necesario, ejecute el siguiente mandato para cambiar los permisos de archivo:

```
chmod a+x package_name.bin
```

en donde *package\_name* es como el siguiente ejemplo:

 Sistemas operativos AIX

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

 Sistemas operativos Linux


```
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

En los ejemplos, *8.1.x.000* representa el nivel de release del producto.

d. Extraiga los archivos de instalación ejecutando el siguiente mandato:

```
./package_name.bin
```

El paquete es grande. Por lo tanto, la extracción tarda un tiempo.

 Sistemas operativos Windows

 Sistemas operativos Windows

a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio, consulte el documento descargado de su producto.

- IBM Spectrum Protect nota técnica 4042944
- IBM Spectrum Protect Extended Edition nota técnica 4042945
- IBM Spectrum Protect for Data Retention nota técnica 4042946

b. Cambie al directorio en el que colocó el archivo ejecutable.

Consejo: En el siguiente paso, los archivos se extraen al directorio actual. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.


c. Para extraer los archivos de instalación, haga doble clic en el archivo ejecutable:


```
package_name.exe
```

Donde *package\_name* es similar al siguiente ejemplo:

```
8.1.x.000-SPSRV-WindowsX64.exe
```

El paquete es grande. Por lo tanto, la extracción tarda un tiempo.

3.  Sistemas operativos AIX Para asegurarse que los asistentes de IBM Spectrum Protect funcionen correctamente, compruebe que esté habilitado el siguiente mandato:


o  Sistemas operativos AIX `lsuser`


De manera predeterminada, el mandato está habilitado.


4. Instale el software de IBM Spectrum Protect haciendo uso de uno de los siguientes métodos. Instale la licencia de IBM Spectrum Protect durante el proceso de instalación.

Consejo: Si tiene varias instancias de servidor en el sistema, instale el software de IBM Spectrum Protect solo una vez para actualizar todas las instancias de servidor.

Asistente de instalación


 Sistemas operativos AIX Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.


 Sistemas operativos Linux Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.


 Sistemas operativos Windows Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.

Asegúrese que su sistema cumpla con los prerrequisitos para usar el asistente de instalación. A continuación, complete el procedimiento de instalación. En la ventana IBM Installation Manager, pulse el icono Update o Modify.

#### Instalación del servidor utilizando la modalidad de consola


 Sistemas operativos AIX Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.


 Sistemas operativos Linux Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.


 Sistemas operativos Windows Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.

Revise la información sobre la instalación del servidor en modalidad de consola y, a continuación, complete el procedimiento de instalación.

#### Modalidad silenciosa

 Sistemas operativos AIX Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.

 Sistemas operativos Linux Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.

 Sistemas operativos Windows Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.




Revise la información sobre la instalación del servidor en modalidad silenciosa y, a continuación, complete el procedimiento de instalación.

Tras instalar el software, no es necesario volver a configurar el sistema.

#### 5. Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.


Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:


- o  Sistemas operativos AIX  Sistemas operativos Linux /var/ibm/InstallationManager/logs
- o  Sistemas operativos Windows C:\ProgramData\IBM\Installation Manager\logs

#### 6. Vaya a IBM Support Portal para obtener arreglos. Pulse Arreglos, actualizaciones y controladores y aplique todo arreglo aplicable.

#### 7. Sistemas operativos AIX Sistemas operativos Linux Verifique que la actualización haya finalizado correctamente:

- a. Inicie la instancia de servidor.

 Sistemas operativos AIX Para obtener instrucciones, consulte Inicio de la instancia de servidor.

 Sistemas operativos Linux Para obtener instrucciones, consulte Inicio de la instancia de servidor.

- b. Supervise los mensajes que el servidor emita al comenzar. Esté atento a los mensajes de error y advertencia, y resuelva cualquier problema.
- c. Compruebe que puede conectarse al servidor mediante el cliente de administración. Para iniciar una sesión de cliente de administración, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:


```
dsmadm
```

- d. Para obtener la información sobre el sistema actualizado, ejecute los mandatos QUERY. Por ejemplo, para obtener información consolidada acerca del sistema, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query system
```

Para obtener información acerca de la base de datos, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query db format=detailed
```

8.  Sistemas operativos Windows Verifique que la actualización haya finalizado correctamente:
- Inicie la instancia del servidor. Para iniciar el servidor desde el directorio predeterminado, C:\Program Files\Tivoli\TSM, ejecute el siguiente mandato administrativo IBM Spectrum Protect:  

```
dsmserv -k server_instance
```




*instancia\_servidor* es el nombre de la instancia del servidor. *Server1* es el nombre predeterminado de la primera instancia del servidor IBM Spectrum Protect.

Si tiene previsto ejecutar el servidor como un servicio bajo la cuenta Sistema local, se debe haber otorgado de forma explícita a la cuenta del sistema local acceso a la base de datos del servidor. Para ver las instrucciones, consulte Inicio del servidor haciendo uso de los servicios de Windows.
  - Supervise los mensajes que el servidor emita al comenzar. Esté atento a los mensajes de error y advertencia, y resuelva cualquier problema.
  - Compruebe que puede conectarse al servidor mediante el cliente de administración. Para iniciar una sesión de cliente de administración, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:  

```
dsmadm
```
  - Para obtener la información sobre el sistema actualizado, ejecute los mandatos QUERY. Por ejemplo, para obtener información consolidada acerca del sistema, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:  

```
query system
```

Para obtener información acerca de la base de datos, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:  

```
query db format=detailed
```
9.  Sistemas operativos AIX  Sistemas operativos Linux Registre las licencias para los componentes del servidor de IBM Spectrum Protect que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:
- ```
register license file=installation_directory/server/bin/component_name.lic
```
- en donde *installation_directory* especifique el directorio en el cual instaló el componente, y *component_name* especifica la abreviatura del componente.
- Por ejemplo, si ha instalado el servidor en el directorio predeterminado, /opt/tivoli/tsm, ejecute el siguiente mandato para registrar la licencia:
- ```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```
- Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:
- ```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```
- Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:
- ```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```
- Restricción:**  
No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:
- o IBM Spectrum Protect for Mail
  - o IBM Spectrum Protect for Databases
  - o IBM Spectrum Protect for ERP
  - o IBM Spectrum Protect for Space Management
- El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.
10.  Sistemas operativos Windows Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:
- ```
register license file=installation_directory\server\component_name.lic
```
- en donde *installation_directory* especifique el directorio en el cual instaló el componente, y *component_name* especifica la abreviatura del componente.
- Por ejemplo, si instaló el servidor en el directorio predeterminado, c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato para registrar la licencia:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmbasic.lic
```

Por ejemplo, si instaló IBM Spectrum Protect Extended Edition en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmee.lic
```

Por ejemplo, si ha instaló IBM Spectrum Protect for Data Retention en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\dataaret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:


- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

11. Opcional: Para instalar un paquete de idiomas adicional, utilice la función de modificar de IBM Installation Manager.
12. Opcional: Para actualizar a una versión más reciente del paquete de idiomas, utilice la función de actualizar de IBM Installation Manager.

Qué hacer a continuación

Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.




 Sistemas operativos Windows Si hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect ejecutando el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es `C:\Program Files\Tivoli\TSM\device\drivers`.

Referencia relacionada:

QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)

QUERY DB (Visualizar información de base de datos)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Actualización del servidor en un entorno en clúster

Para actualizar un servidor a V8.1.3 en un entorno en clúster, debe completar las tareas de preparación e instalación. Los procedimientos varían, dependiendo del sistema operativo y el release.

Procedimiento

Siga el procedimiento para su sistema operativo, release de origen y release de destino:


 Sistemas operativos AIX

Tabla 1. Procedimientos para la actualización del servidor en un entorno en clúster en un sistema operativo AIX

| Release de origen | Release de destino | Procedimiento |
|-------------------|--------------------|---|
| V8.1 | Fixpack V8.1.3 | Aplicación de un fixpack a V8 en un entorno en clúster para AIX |
| V6.3 o V7.1 | V8.1.3 | Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.3 en un entorno en clúster para AIX con una instancia de base de datos compartida
Actualización de V6.3 a V8.1.3 en un entorno en clúster para AIX con instancias de base de datos independientes |
| V5.5, V6.1, V6.2 | V7.1.1 o posterior | IBM Spectrum Protect Proceso de actualización y migración: preguntas más frecuentes |


 Sistemas operativos Linux

Tabla 2. Procedimientos para actualizar el servidor en un entorno en clúster en un sistema operativo Linux

| Release de origen | Release de destino | Procedimiento |
|-------------------|--------------------|---|
| V6.3 o posterior | V8.1.3 | Actualización de un servidor configurado con Tivoli System Automation |



 Sistemas operativos Windows

Tabla 3. Procedimientos para la actualización del servidor en un entorno en clúster en un sistema operativo Windows

| Release de origen | Release de destino | Procedimiento |
|-------------------|--------------------|---|
| V8.1 | Fixpack V8.1.3 | Aplicación de un fixpack a V8 en un entorno en clúster para Windows |
| V6.3 o V7.1 | V8.1.3 | Actualización de V6.3 o V7.1 a V8.1 en un entorno de clúster en Windows |
| V5.5, V6.1, V6.2 | V7.1 o posterior | IBM Spectrum Protect Proceso de actualización y migración: preguntas más frecuentes |

- Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.3 en un entorno en clúster para AIX con una instancia de base de datos compartida
Puede actualizar un servidor de IBM Spectrum Protect de V6.3 o V7.1 a V8.1.3 en un entorno en clúster en AIX con una instancia de base de datos compartida. De esta forma, puede beneficiarse de las nuevas características de IBM Spectrum Protect V8.1.3.
- Actualización de V6.3 a V8.1.3 en un entorno en clúster para AIX con instancias de base de datos independientes
Puede actualizar un servidor de V6.3 a V8.1.3 en un entorno en clúster en AIX con instancias de base de datos independientes. De esta forma, puede aprovechar las nuevas características de V8.1.3.
- Actualización de IBM Spectrum Protect a V8.1.3 en un entorno en clúster for Linux
Para aprovechar las nuevas características de IBM Spectrum Protect, puede actualizar el servidor IBM Spectrum Protect que está instalado en un sistema operativo Linux en un entorno en clúster.
- Actualización de un servidor V6.3 o V7.1 a V8.1.3 en un entorno en clúster para Windows
Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.3.

 Sistemas operativos AIX

Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.3 en un entorno en clúster para AIX con una instancia de base de datos compartida

Puede actualizar un servidor de IBM Spectrum Protect de V6.3 o V7.1 a V8.1.3 en un entorno en clúster en AIX con una instancia de base de datos compartida. De esta forma, puede beneficiarse de las nuevas características de IBM Spectrum Protect V8.1.3.

Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado IBM Spectrum Protect desde un DVD, asegúrese de que el DVD esté disponible. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

Acerca de esta tarea

Utilice el siguiente procedimiento cuando el directorio de instancias DB2 se comparte entre los nodos del clúster. El directorio de instancias DB2 se encuentra en la siguiente ubicación:

```
/home/tsminst1/sqllib
```

Si el directorio de instancias DB2 no se comparte entre nodos, siga las instrucciones en Actualización de V6.3 a V8.1.3 en un entorno en clúster para AIX con instancias de base de datos independientes.

Procedimiento

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad de instantánea, lo que crea una copia de seguridad completa de base de datos sin interrumpir ninguna de las copias de seguridad planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea ejecutando el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```


2. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio, ejecutando el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio, ejecutando el siguiente mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsm serv.opt, que está en el directorio de instancia de servidor.
5. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución. Si está usando supervisión a nivel de la aplicación del servidor IBM Spectrum Protect, use su herramienta para formar clústeres para el recurso de la aplicación dsm serv.
6. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso db2sysc en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

7. En el nodo primario, instale el servidor IBM Spectrum Protect V8.1.3 ejecutando el mandato ./install.sh. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. Después de iniciar el asistente, en la ventana de IBM Installation Manager, pulse el icono Update o Modify.

8. Inicie cada servidor V8.1.3 en el primer plano:

- a. Compruebe que haya iniciado sesión con el ID del propietario de la instancia
- b. Navegue al directorio de la instancia y ejecute el siguiente mandato:

```
/opt/tivoli/tsm/server/bin/dsm serv
```

Espere hasta que vea el indicador de servidor, lo que indica que se ha iniciado el servidor.

9. Detenga el servidor para cada instancia de IBM Spectrum Protect que se esté actualizando. Emita el mandato siguiente:

```
halt
```

Consejo: Debido a que el directorio de instancias de DB2 se comparte entre los nodos del clúster, no es necesario que mueva los recursos compartidos al nodo secundario del clúster.

10. En cada nodo secundario del clúster, siga estos pasos:

- a. Instale el servidor IBM Spectrum Protect V8.1.3 ejecutando el mandato ./install.sh. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. 8.1.
 - i. Si está ejecutando el asistente de instalación, en la ventana de IBM Installation Manager, pulse el icono Update o Modify.
 - ii. Si ejecuta el asistente de instalación, en el panel Credenciales de instancia, deseleccione el recuadro de selección Actualizar esta instancia para cada instancia.
 - iii. Si va a instalar el servidor en modalidad de consola, en la solicitud ¿Desea actualizar esta instancia?, especifique NO para cada una de las instancias.
 - iv. Si va a instalar el servidor en modalidad silenciosa, especifique FALSE para el valor de la variable `user.nombre_instancia_update` para cada una de las instancias.
- b. Asegúrese de que se inicie cada servidor de IBM Spectrum Protect V8.1.3. Si está utilizando supervisión a nivel de la aplicación, utilice la herramienta de agrupación en clústeres para iniciar el servidor.

Para obtener instrucciones sobre cómo iniciar el servidor, consulte Inicio de la instancia de servidor.

11. Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde *installation_directory* especifique el directorio en el cual instaló el componente, y *component_name* especifica la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, /opt/tivoli/tsm, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

Referencia relacionada:


BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

HALT (Concluir el servidor)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX

Actualización de V6.3 a V8.1.3 en un entorno en clúster para AIX con instancias de base de datos independientes

Puede actualizar un servidor de V6.3 a V8.1.3 en un entorno en clúster en AIX con instancias de base de datos independientes. De esta forma, puede aprovechar las nuevas características de V8.1.3.

Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado IBM Spectrum Protect desde un DVD, asegúrese de que el DVD esté disponible. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

Acerca de esta tarea

Utilice el siguiente procedimiento cuando la instancia del directorio de DB2 no se comparta entre los nodos en el clúster. El directorio de la instancia de DB2 se encuentra en la siguiente ubicación:

```
/home/tsminst1/sqllib
```

Si la instancia del directorio de DB2 se comparten entre los nodos del clúster, siga las instrucciones en Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.3 en un entorno en clúster para AIX con una instancia de base de datos compartida.

Procedimiento

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad de instantánea, lo que crea una copia de seguridad completa de base de datos sin interrumpir ninguna de las copias de seguridad planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea ejecutando el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio, ejecutando el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio, ejecutando el siguiente mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado `dsmserv.opt`, que está en el directorio de instancia de servidor.
5. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución. Si está usando supervisión a nivel de la aplicación del servidor IBM Spectrum Protect, use su herramienta para formar clústeres para el recurso de la aplicación `dsmserv`.
6. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso `db2sysc` en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

7. Asegúrese de que todos los recursos compartidos para todas las instancias de IBM Spectrum Protect se encuentren en el nodo primario. Verifique que ningún otro nodo tenga acceso de grabación sobre estos recursos durante la actualización. Si el entorno incluya varias instancias del servidor, el nodo primario debe poder acceder a los recursos compartidos para todas las instancias.
8. En el nodo primario, instale el servidor V8.1.3 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. Después de iniciar el asistente, en la ventana de IBM Installation Manager, pulse el icono **Install**; no pulse el icono **Update** o **Modify**. Para completar la actualización de V6.3 a V8.1.3, tiene que instalar el servidor V8.1.3.
9. Inicie cada servidor V8.1.3 en el primer plano:
 - a. Compruebe que haya iniciado sesión con el ID del propietario de la instancia
 - b. Navegue al directorio de la instancia y ejecute el siguiente mandato:

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Espere hasta que vea el indicador de servidor, lo que indica que se ha iniciado el servidor.

10. Detenga el servidor para cada instancia de IBM Spectrum Protect que se esté actualizando. Ejecute este mandato:

```
halt
```

11. En cada nodo secundario del clúster, siga estos pasos:
 - a. Mueva todos los recursos compartidos al nodo secundario. Si el entorno incluye varias instancias del servidor, el nodo secundario debe poder acceder a los recursos compartidos para todas las instancias durante la actualización.
 - b. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución.
 - c. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso `db2sysc` en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

- d. Instale el servidor V8.1.3 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor.
 - i. Si va a utilizar el asistente de instalación, en la ventana IBM Installation Manager, pulse sobre el icono **Instalar**; no pulse sobre el icono **Actualizar** ni sobre el icono **Modificar**.
 - ii. Si está utilizando el asistente de instalación, en la página **Credenciales de instancia**, seleccione el recuadro de selección **Configurar esta instancia en un nodo secundario del clúster** para cada instancia que está configurando.
 - iii. Si va a instalar el servidor en modalidad de consola, en la solicitud `¿Desea configurar esta instancia en un nodo secundario del clúster?`, especifique **YES (S)** para cada una de las instancias.
 - iv. Si va a instalar el servidor en modalidad silenciosa, especifique **TRUE** para el valor de la variable `user.nombre_instancia_secondaryNode` para cada una de las instancias.
- e. Asegúrese de que se inicia cada servidor V8.1.3. Si está utilizando supervisión a nivel de la aplicación, utilice la herramienta de agrupación en clústeres para iniciar el servidor.

Para obtener instrucciones sobre cómo iniciar el servidor, consulte **Inicio de la instancia de servidor**.

12. Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato **REGISTER LICENSE**:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde *installation_directory* especifique el directorio en el cual instaló el componente, y *component_name* especifique la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, `/opt/tivoli/tsm`, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

Referencia relacionada:

BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

HALT (Concluir el servidor)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos Linux

Actualización de IBM Spectrum Protect a V8.1.3 en un entorno en clúster for Linux

Para aprovechar las nuevas características de IBM Spectrum Protect, puede actualizar el servidor IBM Spectrum Protect que está instalado en un sistema operativo Linux en un entorno en clúster.

Procedimiento

Siga las instrucciones de Configuración de un entorno de Linux para la agrupación en clúster.

 Sistemas operativos Windows

Actualización de un servidor V6.3 o V7.1 a V8.1.3 en un entorno en clúster para Windows

Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.3.

Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado el servidor desde un paquete descargado, asegúrese de que los archivos descargados están disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

Procedimiento

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad instantánea, que proporciona una copia de seguridad completa de la base de datos sin interrumpir las copias de seguridad programadas. Por ejemplo, puede ejecutar el siguiente mandato para crear una copia de seguridad de instantánea:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo a otro directorio. Ejecute el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio. Ejecute este mandato:

backup volhistory filenames=*nombre_archivo*

donde *nombre_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt, que está en el directorio de instancia de servidor.
5. Asegúrese de que el grupo de recursos esté en el nodo primario y de que todos los nodos del clúster se estén ejecutando. Realice las acciones siguientes en el nodo primario:
 - a. En la ventana Gestor de clúster de migración, desactive el recurso del servidor y elimínelo:
 - i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor se mostrará en la sección Otros recursos.
 - ii. Seleccione el recurso del servidor y pulse Desactivar este recurso.
 - iii. Para suprimir el recurso del servidor, selecciónelo y pulse Suprimir.
 - b. En la ventana Gestor de clúster de migración tras error, suprima el nombre de red y la dirección IP:
 - i. En la sección Nombre del servidor, expanda el nombre de la red para ver la dirección IP. Anote el nombre de la red y la dirección IP.
 - ii. Seleccione el nombre de la red y la dirección IP, y pulse Eliminar.
 - c. En la ventana Gestor de clúster de migración, desactive el recurso del servidor DB2:
 - i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor de IBM Spectrum Protect se mostrará en la sección Otros recursos.
 - ii. Seleccione un recurso del servidor DB2, por ejemplo, SERVER1, y pulse Desactivar este recurso.
6. Asegúrese de que el servidor se esté ejecutando en el nodo primario. Realice los pasos siguientes en todos los demás nodos del clúster:
 - a. Instale el servidor IBM Spectrum Protect V8.1.3.
 - b. Detenga el servicio de clúster. Una forma de detenerlo es utilizando la aplicación de servicio. Pulse con el botón derecho sobre Servicio de clúster y seleccione Detener.
 - c. Suprima los archivos tsmsvrrscexX64.dll y tsmsvrrscx64.dll del directorio C:\Windows\Cluster.
 - d. Copie los archivos DLL siguientes del directorio de instalación en el directorio C:\Windows\Cluster:
 - tsmsvrrscexX64.dll
 - tsmsvrrscx64.dll
 - e. Copie el archivo DLL siguiente del directorio de instalación en el directorio C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
 - f. Inicie el servicio de clúster. Una forma de iniciarlo es utilizando la aplicación de servicio. Pulse con el botón derecho del ratón sobre Servicio de clúster y seleccione Inicio.
7. En el Administrador de clústeres de migración tras error, mueva la instancia del servidor IBM Spectrum Protect desde el nodo primario a otro nodo del clúster.
8. Realice los pasos siguientes en el nodo primario:
 - a. Instale el servidor IBM Spectrum Protect V8.1.3.
 - b. Detenga el servicio de clúster.
 - c. Suprima los archivos tsmsvrrscexX64.dll y tsmsvrrscx64.dll del directorio C:\Windows\Cluster.
 - d. Copie los archivos DLL siguientes del directorio de instalación en el directorio C:\Windows\Cluster:
 - tsmsvrrscexX64.dll
 - tsmsvrrscx64.dll
 - e. Copie el archivo DLL siguiente del directorio de instalación en el directorio C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
 - f. Inicie el servicio de clúster.
9. Opcional: Vuelva a mover la instancia del servidor IBM Spectrum Protect al nodo primario.

Qué hacer a continuación

Si hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos disponible, instale el controlador de dispositivos de IBM Spectrum Protect ejecutando el mandato dpinst.exe /a. El archivo dpinst.exe se encuentra en el directorio del controlador de dispositivos y la ubicación predeterminada es C:\Program Files\Tivoli\TSM\device\drivers.




Referencia relacionada:

BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalación y actualización del Centro de operaciones

IBM Spectrum Protect Operations Center es la interfaz basada en web para gestionar el entorno de almacenamiento.

Antes de empezar

Antes de instalar y configurar el Centro de operaciones, revise la siguiente información:

- Requisitos del sistema del Centro de operaciones
 - Requisitos de sistema del Centro de operaciones
 - Requisitos del servidor concentrador y spoke
 - Requisitos de sistema operativo
 - Requisitos del navegador web
 - Requisitos de idioma
 - Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect
- Los ID de administrador que requiere el centro de operaciones
- IBM Installation Manager
- Lista de comprobación de la instalación
- Obtención del paquete de instalación de Centro de operaciones



Acerca de esta tarea

Tabla 1 enumera los métodos para instalar o desinstalar Centro de operaciones e indica en dónde encontrar las instrucciones relacionadas.

Para obtener información sobre la actualización de Centro de operaciones, consulte Actualización del Centro de operaciones.

Tabla 1. Métodos para instalar o desinstalar Centro de operaciones

| comunicaciones | Instrucciones |
|----------------------|--|
| Asistente gráfico | <ul style="list-style-type: none">• Instalación de Centro de operaciones utilizando el asistente gráfico• Desinstalación de Centro de operaciones utilizando el asistente gráfico |
| Modalidad de consola | <ul style="list-style-type: none">• Instalar el Centro de operaciones en modalidad de consola• Desinstalación del Centro de operaciones en modalidad de consola |
| Modalidad silenciosa | <ul style="list-style-type: none">• Instalación de Centro de operaciones en el modo silencioso• Desinstalar Centro de operaciones en modalidad silenciosa |

- Planificación para instalar el Centro de operaciones
Antes de instalar Centro de operaciones, debe entender los requisitos del sistema, los ID de administrador que requiere Centro de operaciones y la información que debe proporcionarle al programa de instalación.
- Instalar el Centro de operaciones
Puede instalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Actualización del Centro de operaciones
Puede actualizar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.
- Guía de inicio de la Centro de operaciones
Antes de poder utilizar Centro de operaciones para gestionar el entorno de almacenamiento, debe configurarlo.
-  Sistemas operativos AIX  Sistemas operativos Linux Resolución de problemas de la instalación de Centro de operaciones
Si ocurre un problema con la instalación del Centro de operaciones y no puede resolverlo, puede consultar las descripciones de problemas conocidos para una posible solución.
- Desinstalación de Centro de operaciones
Puede desinstalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Volver a una versión anterior de Centro de operaciones
De forma predeterminada, IBM Installation Manager guarda versiones anteriores de un paquete para poder regresar a una versión anterior si experimenta un problema con versiones posteriores de actualizaciones, arreglos o paquetes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Planificación para instalar el Centro de operaciones

Antes de instalar Centro de operaciones, debe entender los requisitos del sistema, los ID de administrador que requiere Centro de operaciones y la información que debe proporcionarle al programa de instalación.

Acerca de esta tarea

Desde Centro de operaciones, puede gestionar los siguientes aspectos principales del entorno de almacenamiento:

- servidores y clientes de IBM Spectrum Protect
- Servicios como copia de seguridad y restauración, archivar y restablecer y migrar y recuperar
- Agrupaciones de almacenamiento y dispositivos de almacenamiento

Centro de operaciones incluye las funciones siguientes:

Interfaz de usuario para varios servidores

Puede usar Centro de operaciones para gestionar uno o más servidores IBM Spectrum Protect.

En un entorno con varios servidores, puede designar un servidor como un *servidor concentrador* y los otros como *servidores de radio*. El servidor central puede recibir alertas e información del estado desde los servidores de radio y presentar la información de manera consolidada en Centro de operaciones.

Supervisor de alertas




Una *alerta* es una notificación de un problema importante en el servidor y se desencadena mediante un mensaje de servidor. Puede definir qué mensajes del servidor se envían como alertas, y sólo esos mensajes se clasifican como alertas en Centro de operaciones o en un correo electrónico.

Esta supervisión de la alerta puede ayudarle a identificar y rastrear problemas importantes en el servidor.

Interfaz conveniente de la línea de mandatos

Centro de operaciones incluye una interfaz de línea de mandatos para configuración y características avanzadas.

- Requisitos del sistema del Centro de operaciones
Antes de instalar el Centro de operaciones, asegúrese de que su sistema cumple con los requisitos mínimos.
- Los ID de administrador que requiere el centro de operaciones
Un administrador debe tener un ID y contraseña válidos en el servidor hub para iniciar sesión en el Centro de operaciones. Un ID de administrador también se asigna al Centro de operaciones para que el Centro de operaciones pueda gestionar los servidores.
- IBM Installation Manager
El Centro de operaciones utiliza el IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- Lista de comprobación de la instalación
Antes de instalar Centro de operaciones, debe verificar cierta información, como las credenciales de instalación y debe determinar la información de entrada que debe proporcionarle a IBM Installation Manager para la instalación.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Requisitos del sistema del Centro de operaciones

Antes de instalar el Centro de operaciones, asegúrese de que su sistema cumple con los requisitos mínimos.

Utilice la Calculadora de requisitos del sistema del Centro de operaciones para realizar una estimación de los requisitos del sistema para ejecutar el Centro de operaciones y los servidores concentrador y de radio que supervisa el Centro de operaciones.

Requisitos que se verifican durante la instalación

Tabla 1 enumera los requerimientos que son un prerrequisito y que se verifican durante la instalación e indica en dónde encontrar más información sobre estos requerimientos.

Tabla 1. Requisitos que se verifican durante la instalación

| Requisito | Detalles |
|---|---|
| Requisito mínimo de memoria | Requisitos de sistema del Centro de operaciones |
| Requisito del sistema operativo | Requisitos de sistema operativo |
| Nombre de host del sistema en el que se instalará Centro de operaciones | Lista de comprobación de la instalación |
| Requisitos para el directorio de instalación de Centro de operaciones | Lista de comprobación de la instalación |

- Requisitos de sistema del Centro de operaciones
Puede instalar Centro de operaciones en un sistema que también está ejecutando el servidor IBM Spectrum Protect o en un

sistema diferente. Si instala Centro de operaciones en el mismo sistema que un servidor, dicho sistema debe cumplir los requisitos del sistema para ambos, Centro de operaciones y el servidor.

- Requisitos del servidor concentrador y spoke
Cuando se abre el centro de operaciones por primera vez, es necesario asociarlo a un servidor de IBM Spectrum Protect designado como *servidor concentrador*. En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Requisitos de sistema operativo
El Centro de operaciones está disponible para los sistemas de AIX, Linux y Windows.
- Requisitos del navegador web
Centro de operaciones puede ejecutarse en los navegadores web Apple, Google, Microsoft, y Mozilla.
- Requisitos de idioma
De forma predeterminada, el Centro de operaciones utiliza el idioma que utiliza el navegador web. Sin embargo, el proceso de instalación utiliza el idioma que utiliza el sistema operativo. Compruebe que el navegador web y el sistema operativo estén establecidos en el idioma que necesita.
- Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect
servicios de gestión de cliente de IBM Spectrum Protect es un componente que se instala en clientes de archivado y copia de seguridad para recopilar información de diagnóstico como, por ejemplo, archivos de registro de cliente. Antes de instalar el servicio de gestión de clientes en el sistema, debe conocer los requisitos y las limitaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Requisitos de sistema del Centro de operaciones

Puede instalar Centro de operaciones en un sistema que también está ejecutando el servidor IBM Spectrum Protect o en un sistema diferente. Si instala Centro de operaciones en el mismo sistema que un servidor, dicho sistema debe cumplir los requisitos del sistema para ambos, Centro de operaciones y el servidor.

Requisitos de recursos

Se requieren los siguientes recursos para ejecutar el Centro de operaciones:

- Un núcleo de procesador
- 4 GB de memoria
- 1 GB de espacio en disco

El servidor de radio y el servidor central que supervisa el Centro de operaciones requiere recursos adicionales, según se describe en Requisitos del servidor concentrador y spoke.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Requisitos del servidor concentrador y spoke

Cuando se abre el centro de operaciones por primera vez, es necesario asociarlo a un servidor de IBM Spectrum Protect designado como *servidor concentrador*. En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

Si Centro de operaciones solo supervisa un servidor, dicho servidor se sigue denominando servidor concentrador, aunque no tenga conectado ningún servidor de radio.

Tabla 1 indica la versión del servidor IBM Spectrum Protect que debe instalarse en el servidor concentrador y en cada servidor spoke que es gestionado por Centro de operaciones.




Tabla 1. IBM Spectrum Protect requisitos de la versión del servidor para el servidor hub y el servidor de radio

| Centro de operaciones | Versión en el servidor concentrador | Versión en cada servidor de radio |
|-----------------------|-------------------------------------|--|
| V8.1.3 | V8.1.3 | V6.3.4 o posteriores
Restricción: Algunas funciones de Centro de operaciones no están disponibles para los servidores que utilicen una versión anterior a V8.1.3. |

Número de servidores spoke que un servidor concentrador puede admitir

El número de servidores spoke que un servidor concentrador puede soportar depende de la configuración y de la versión de IBM Spectrum Protect en cada servidor spoke. Sin embargo, una guía general es que el servidor concentrador puede admitir de 10 a 20 servidores spoke V6.3.4, pero puede admitir más servidores spoke V7.1 o posteriores.

- Consejos para designar la configuración del servidor concentrador y el servidor de radio
Al diseñar la configuración central y de radio, considere especialmente los requisitos de recursos para la supervisión del estado. También, considere cómo quiere agrupar los servidores centrales y de radio y si quiere usar varios servidores centrales.
- Consejos para elegir un servidor concentrador
Para el servidor concentrador, debe elegir un servidor que tenga los recursos adecuados y que se encuentre para una latencia de red de viaje de ida y vuelta mínima.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Consejos para designar la configuración del servidor concentrador y el servidor de radio

Al diseñar la configuración central y de radio, considere especialmente los requisitos de recursos para la supervisión del estado. También, considere cómo quiere agrupar los servidores centrales y de radio y si quiere usar varios servidores centrales.

Utilice la Calculadora de requisitos del sistema del Centro de operaciones para realizar una estimación de los requisitos del sistema para ejecutar el Centro de operaciones y los servidores concentrador y de radio que supervisa el Centro de operaciones.

Factores principales que afectan al rendimiento

Los factores siguientes tienen mayor impacto en el rendimiento del Centro de operaciones:

- El procesador y la memoria del sistema en el que está instalado el Centro de operaciones
- Los recursos del sistema del servidor concentrador y los servidores de radio, incluyendo el sistema de disco que está en uso para la base de datos del servidor concentrador
- El número de nodos de cliente y espacios de archivos de máquina virtual gestionados por los servidores concentrador y de radio.
- La frecuencia a la cual se renuevan los datos en Centro de operaciones

Cómo agrupar los servidores concentradores y de radio

Tenga en cuenta agrupar los servidores concentradores y de radio por ubicación geográfica. Por ejemplo, la gestión de los servidores dentro del mismo centro de datos puede ayudar a impedir problemas provocados por los cortafuegos o por un ancho de banda de red inadecuado entre las distintas ubicaciones. Si fuera necesario, puede dividir los servidores según una o más de las siguientes características:

- El administrador que gestiona los servidores
 - La entidad de organización que funda los servidores
 - Sistema operativo del servidor
 - El idioma en que se ejecutan los servidores
- Consejo: Si los servidores concentradores y de radio no se están ejecutando en el mismo idioma, podría ver texto corrupto en el Centro de operaciones.

Cómo agrupar servidores concentradores y de radio en una configuración empresarial

En una configuración empresarial, una red de servidores de IBM Spectrum Protect se gestiona como un grupo. Los cambios que se realizan en el *gestor de configuración* se pueden distribuir automáticamente en uno o más *servidores gestionados* de la red.

Normalmente el Centro de operaciones registra y mantiene un ID de administrador dedicado en los servidores concentradores y de radio. Este *administrador de supervisión* debe tener siempre la misma contraseña en todos los servidores.

Si utiliza una configuración empresarial, puede mejorar el proceso mediante el cual las credenciales de administrador se sincronizan en los servidores de radio. Para mejorar el rendimiento y la eficiencia de mantener el ID de administrador de supervisión, realice los pasos siguientes:

1. Designe el servidor de gestor de configuración como servidor concentrador del Centro de operaciones. Durante la configuración del servidor concentrador, se registra un ID de administrador de supervisión denominado IBM-OC-*nombre_servidor_concentrador*.

2. En el servidor concentrador, añada el ID de administrador de supervisión a un perfil de configuración empresarial nuevo o existente. Emita el mandato NOTIFY SUBSCRIBERS para distribuir el perfil a los servidores gestionados.
3. Añada uno o más de los servidores gestionados como servidores de radio del Centro de operaciones.




El Centro de operaciones detecta esta configuración y permite al gestor de configuración distribuir y actualizar el ID de administrador de supervisión en los servidores de radio.

Cuándo usar varios servidores concentradores

Si tiene más de 10 - 20 servidores de radio V6.3.4, o si las limitaciones de recursos requieren que se particione el entorno, puede configurar varios servidores concentradores y conectar un subconjunto de servidores de radio a cada servidor concentrador.

Restricciones:

- Un único servidor no puede utilizarse como servidor hub y servidor spoke.
- Cada servidor spoke puede asignarse a un único servidor hub.
- Cada servidor hub necesita una instancia independiente de Centro de operaciones, con una dirección web separada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Consejos para elegir un servidor concentrador

Para el servidor concentrador, debe elegir un servidor que tenga los recursos adecuados y que se encuentre para una latencia de red de viaje de ida y vuelta mínima.

Atención: No utilice el mismo servidor como servidor concentrador para varios centros de operaciones.

Utilice las directrices siguientes para decidir qué servidor designar como servidor concentrador:

Elija un servidor con carga ligera

Considere un servidor que tenga una carga ligera para operaciones como, por ejemplo, copia de seguridad y archivado de cliente. Un servidor con carga ligera es también una buena opción como sistema host para el Centro de operaciones.

Asegúrese de que el servidor tiene los recursos para manejar tanto su carga de trabajo de servidor típica y la carga de trabajo estimada para actuar como servidor concentrador.

Ubique el servidor para obtener una latencia de red de ida y vuelta mínima

Ubique el servidor concentrador de manera que la conexión de red entre el servidor concentrador y los servidores de radio tenga una latencia de viaje de ida y vuelta que no sea superior a 5 ms. Esta latencia puede conseguirse habitualmente cuando los servidores están en la misma red de área local (LAN).

Las redes mal ajustadas, que sean muy utilizadas por otras aplicaciones, o que tengan una latencia de ida y vuelta mucho mayor que 5 ms, pueden degradar las comunicaciones entre los servidores de radio y concentrador. Por ejemplo, una latencia de ida y vuelta de 50 ms o superior puede resultar en tiempos de comunicación que hagan que los servidores de radio se desconecten o vuelvan a conectar al Centro de operaciones. Estas altas latencias pueden experimentarse en comunicaciones de red área amplia (WAN) de larga distancia.

Si los servidores de radio están a gran distancia del servidor concentrador y experimentan desconexiones frecuentes en el Centro de operaciones, puede aumentar el valor de la opción ADMINCOMMTIMEOUT en cada servidor para atenuar el problema.

Verifique que el servidor concentrador cumple los requisitos de recurso de supervisión de estado

La supervisión de estado requiere recursos adicionales en cada servidor en los que está habilitada. Los recursos necesarios dependen principalmente del número de clientes gestionados por los servidores concentrador y de radio. Se utilizan menos recursos en un servidor concentrador con un servidor spoke V7.1 o posterior que en un servidor concentrador con un servidor spoke V6.3.4.

Compruebe que el servidor concentrador cumple los requisitos de recurso de uso de procesador, espacio de base de datos, espacio de registro de archivado y capacidad de operaciones de E/S por segundo (IOPS).




Un servidor concentrador con una capacidad de IOPS alta puede manejar una mayor cantidad de datos de estado entrantes de los servidores de radio. El uso de los dispositivos de almacenamiento siguientes para la base de datos del servidor concentrador puede ayudarle a alcanzar esta capacidad:

- Una unidad de estado sólido (SSD) de nivel de empresa
- Un dispositivo de almacenamiento de disco SAN externo con varios volúmenes o varios pernos en cada volumen

En un entorno con menos de 1000 clientes, considere establecer una capacidad de línea de base de 1000 IOPS para la base de datos del servidor concentrador si el servidor concentrador gestiona cualquier servidor de radio.

Determine si el entorno requiere varios servidores concentradores



Si hay más de 10.000 - 20.000 nodos de cliente y espacios de archivos de máquina virtual gestionados por un conjunto de servidores concentrador y de radio, los requisitos de recurso podrían exceder lo que tiene disponible el servidor concentrador, especialmente, si los servidores de radio son servidores V6.3.4. Plantéese designar un segundo servidor como servidor concentrador y trasladar los servidores de radio al servidor concentrador nuevo para equilibrar la carga.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




Requisitos de sistema operativo

El Centro de operaciones está disponible para los sistemas de AIX, Linux y Windows.

Puede ejecutar Centro de operaciones en los siguientes sistemas:

-  Sistemas operativos AIXSistemas AIX:
 - IBM® AIX V7.1 (64 bits) TL 4 y SP 2
 - IBM AIX V7.2 (64 bits) TL 0 y SP 2
-  Sistemas operativos LinuxLinux en sistemas x86_64:
 - Red Hat Enterprise Linux 6.7
 - Red Hat Enterprise Linux 7.1
 - SUSE Linux Enterprise Server 11, Service Pack 4 o posterior
 - SUSE Linux Enterprise Server 12
-  Sistemas operativos LinuxSistemas Linux on System z (arquitectura s390x de 64 bits):
 - Red Hat Enterprise Linux 7.1
 - SUSE Linux Enterprise Server 12
-  Sistemas operativos LinuxSistemas Linux on Power Systems (little endian):
 - Red Hat Enterprise Linux 7 con la arquitectura PPC64LE
-  Sistemas operativos WindowsSistemas Windows:
 - Microsoft Windows Server 2012: Standard, Enterprise o Datacenter Edition (64 bits)
 - Microsoft Windows Server 2012 R2 (64 bits)
 - Microsoft Windows Server 2016

Para obtener la información más actualizada sobre requisitos, consulte Requisitos de software y hardware.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Requisitos del navegador web

Centro de operaciones puede ejecutarse en los navegadores web Apple, Google, Microsoft, y Mozilla.

Para obtener una vista óptima de Centro de operaciones en el navegador web, asegúrese de que la resolución en pantalla del sistema esté configurada en un mínimo de 1024 X 768 píxeles.

Para obtener un rendimiento óptimo, utilice un navegador web que tenga un buen rendimiento de JavaScript y habilite el almacenamiento en memoria caché del navegador.

Centro de operaciones puede ejecutarse en los siguientes navegadores web:

- Apple Safari en el iPad
Restricción: Si Apple Safari se está ejecutando en iOS 8.x o iOS 9.x, no puede utilizar un certificado firmado automáticamente para la comunicación segura con el Centro de operaciones sin una configuración adicional del certificado. Utilice un certificado de entidad emisora de certificados (CA) o configure el certificado autofirmado como sea necesario. Para obtener instrucciones, consulte la nota técnica <http://www.ibm.com/support/docview.wss?uid=swg21963153>.
- Google Chrome 40 o posterior
- Microsoft Internet Explorer 11 o posterior
- Mozilla Firefox ESR 31 o posterior

Para ejecutar el Centro de operaciones en conformidad con la recomendación 800-131A para Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST), la comunicación entre el Centro de operaciones y el navegador web debe protegerse utilizando el protocolo TLS (Seguridad de la capa de transporte) 1.2. Durante la instalación, especifique si la conformidad 800-131A de SP es necesaria y el nivel de conformidad. Si durante la instalación se especifica conformidad 800-131A de SP estricta, el navegador web debe soportar TLS 1.2 y se debe habilitar TLS 1.2.

El navegador web visualiza un error de SSL si se especifica el cumplimiento estricto de SP 800-131A durante la instalación y el navegador web no cumple los requisitos anteriores.

Requisitos de idioma

De forma predeterminada, el Centro de operaciones utiliza el idioma que utiliza el navegador web. Sin embargo, el proceso de instalación utiliza el idioma que utiliza el sistema operativo. Compruebe que el navegador web y el sistema operativo estén establecidos en el idioma que necesita.


 Sistemas operativos AIX

Tabla 1. Centro de operaciones valores de idioma que puede usar en los sistemas AIX

| Idioma | Valor opción LANGUAGE |
|-----------------------------|-----------------------|
| Chino simplificado | zh_CN |
| Chino, simplificado (UTF-8) | ZH_CN |
| Chino, tradicional (Big5) | Zh_TW |
| Chino, tradicional (UTF-8) | ZH_TW |
| Chino tradicional (euc_tw) | zh_TW |
| Inglés | en_US |
| Inglés (UTF-8) | EN_US |
| Francés | fr_FR |
| Francés (UTF-8) | FR_FR |
| Alemán | de_DE |
| Alemán (UTF-8) | DE_DE |
| Italiano | it_IT |
| Italiano (UTF-8) | IT_IT |
| Japonés (EUC) | ja_JP |
| Japonés (PC) | Ja_JP |
| Japonés (UTF-8) | JA_JP |
| Coreano | ko_KR |
| Coreano (UTF-8) | KO_KR |
| Portugués, Brasileño | pt_BR |
| Portugués de Brasil (UTF-8) | PT_BR |
| Ruso | ru_RU |
| Ruso (UTF-8) | RU_RU |
| Español | es_ES |
| Español (UTF-8) | ES_ES |


 Sistemas operativos Linux

Tabla 2. Centro de operaciones valores de idioma que puede usar en los sistemas Linux

| Idioma | Valor opción LANGUAGE |
|-----------------------------|-----------------------|
| Chino simplificado | zh_CN |
| Chino simplificado (GBK) | zh_CN.gb18030 |
| Chino, simplificado (UTF-8) | zh_CN.utf8 |
| Chino, tradicional (Big5) | Zh_TW |
| Chino, tradicional (euc_tw) | zh_TW |
| Chino, tradicional (UTF-8) | zh_TW.utf8 |
| Inglés de Estados Unidos | en_US |

| Idioma | Valor opción LANGUAGE |
|------------------------------|-----------------------|
| Inglés (UTF-8) | en_US.utf8 |
| Francés | fr_FR |
| Francés (UTF-8) | fr_FR.utf8 |
| Alemán | de_DE |
| Alemán (UTF-8) | de_DE.utf8 |
| Italiano | it_IT |
| Italiano (UTF-8) | it_IT.utf8 |
| Japonés (EUC) | ja_JP |
| Japonés (UTF-8) | ja_JP.utf8 |
| Coreano | ko_KR |
| Coreano (UTF-8) | ko_KR.utf8 |
| Portugués, Brasileño | pt_BR |
| Portugués, de Brasil (UTF-8) | pt_BR.utf8 |
| Ruso | ru_RU |
| Ruso (UTF-8) | ru_RU.utf8 |
| Español | es_ES |
| Español (UTF-8) | es_ES.utf8 |





 Sistemas operativos Windows

Tabla 3. Centro de operaciones valores de idioma que puede usar en los sistemas Windows

| Idioma | Valor opción LANGUAGE |
|----------------------|-----------------------|
| Chino simplificado | chs |
| Chino, Tradicional | cht |
| Inglés | ameng |
| Francés | fra |
| Alemán | deu |
| Italiano | ita |
| Japonés (Shift-JIS) | jpn |
| Coreano | kor |
| Portugués, Brasileño | ptb |
| Ruso | rus |
| Español | esp |

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect

servicios de gestión de cliente de IBM Spectrum Protect es un componente que se instala en clientes de archivado y copia de seguridad para recopilar información de diagnóstico como, por ejemplo, archivos de registro de cliente. Antes de instalar el servicio de gestión de clientes en el sistema, debe conocer los requisitos y las limitaciones.

En la documentación de servicio de gestión de clientes, *sistema cliente* es el sistema donde está instalado el cliente de archivado y copia de seguridad.

La información de diagnóstico se puede recopilar solo desde clientes Linux y Windows. pero los administradores pueden ver la información de diagnóstico en Centro de operaciones en sistemas operativos AIX, Linux o Windows.

Requisitos para el servicio de gestión de clientes

Compruebe los siguientes requisitos antes de instalar servicio de gestión de clientes:

- Para acceder de forma remota al cliente, el administrador del Centro de operaciones debe tener autoridad de sistema y uno de los siguientes niveles de autoridad de cliente:
 - Autoridad de política
 - Autoridad de propietario de cliente
 - Autoridad de acceso de nodo de cliente
- Asegúrese de que el sistema cliente cumple estos requisitos:
 - El servicio de gestión de clientes solo se puede instalar en sistemas cliente que se ejecutan en sistemas operativos Linux o Windows:
 - Sistemas operativos Linux x86 de 64 bits soportados para el cliente de archivado y copia de seguridad.
 - Sistemas operativos Windows de 32 bits y de 64 bits soportados para el cliente de archivado y copia de seguridad.
 - Debe instalarse TLS (seguridad de la capa de transporte) 1.2 para la transmisión de datos entre servicio de gestión de clientes y Centro de operaciones. Se proporciona autenticación básica y los datos y la información de autenticación se cifran a través del canal SSL. TLS 1.2 se instala de forma automática junto con los certificados SSL necesarios al instalar el servicio de gestión de clientes.
- En los sistemas cliente Linux, debe tener autorización de usuario root para instalar servicio de gestión de clientes.
- Para los sistemas cliente que puede tener varios nodos de cliente, como los sistemas clientes de Linux, asegúrese de que cada nombre de nodo sea exclusivo en el sistema cliente.
Consejo: Después de instalar el servicio de gestión de clientes, no tiene que instalarlo otra vez porque el servicio puede descubrir varios archivos de opciones de cliente.

Limitaciones de servicio de gestión de clientes




servicio de gestión de clientes proporciona los servicios básicos para recopilar información de diagnóstico de los clientes de archivado y copia de seguridad. Existen las siguientes limitaciones para servicio de gestión de clientes:

- Puede instalar servicio de gestión de clientes solo en sistemas con clientes de archivado y copia de seguridad, incluidos los clientes de archivado y copia de seguridad que están instalados en nodos de transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
- No puede instalar servicio de gestión de clientes en otros productos o componentes de cliente IBM Spectrum Protect que no tengan clientes de copia de seguridad/archivado.
- Si los clientes de archivado y copia de seguridad están protegidos mediante un cortafuegos, asegúrese de que el Centro de operaciones se puede conectar a los clientes de archivado y copia de seguridad a través del cortafuegos utilizando el puerto configurado para servicio de gestión de clientes. El puerto predeterminado es el 9028, pero no se puede cambiar.
- El cliente de servicio de gestión de clientes lee todos los archivos de registro para localizar entradas para el periodo anterior de 72 horas.
- La página Diagnóstico de Centro de operaciones proporciona información de resolución de problemas básica de los clientes de archivado y copia de seguridad. Sin embargo, para algunos problemas de copia de seguridad, es posible que tenga que acceder al sistema cliente y obtener información de diagnóstico adicional.
- Si el tamaño combinado de los archivos de registro de errores de cliente y de los archivos de registro de planificación es superior a 500 MB, se pueden producir retardos al enviar registros de anotaciones al Centro de operaciones. Puede controlar el tamaño de los archivos de registro habilitando la depuración o el ajuste de los archivos de registro especificando la opción de cliente errorlogretention o errorlogmax.
- Si utiliza el mismo nombre de nodo de cliente para conectarse a varios servidores de IBM Spectrum Protect que están instalados en el mismo servidor, solo puede ver los archivos de registro para uno de los nodos de cliente.

Para obtener las actualizaciones con respecto a servicio de gestión de clientes, incluyendo requisitos, limitaciones y actualizaciones de documentación, consulte la nota técnica 1963610.

Tareas relacionadas:

Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Los ID de administrador que requiere el centro de operaciones

Un administrador debe tener un ID y contraseña válidos en el servidor hub para iniciar sesión en el Centro de operaciones. Un ID de administrador también se asigna al Centro de operaciones para que el Centro de operaciones pueda gestionar los servidores.

Centro de operaciones requiere los siguientes ID de administrador IBM Spectrum Protect:

Los ID de administrador que están registrados en el servidor central

Cualquier ID de administrador de que está registrado en el servidor hub puede utilizarse para iniciar sesión en el Centro de operaciones. El nivel de autorización del ID determina las tareas que pueden completarse. Para crear IDs de administrador, utilice el mandato REGISTER ADMIN.

Restricción: Para utilizar un ID de administrador en una configuración de varios servidores, el ID debe estar registrado en los servidores centrales y de radio con la misma contraseña y nivel de autorización.

Para gestionar la autenticación de estos servicios, considere utilizar uno de los siguientes métodos:

- Un servidor LDAP(Lightweight Directory Access Protocol)
- Las funciones de configuración empresarial para distribuir automáticamente los cambios en las definiciones de administrador.

Supervisión del ID de administrador




Cuando configura el servidor hub de forma inicial, un ID de administrador llamado IBM-OC-*server_name* se registra con autoridad de sistema en el servidor hub y se asocia a la contraseña inicial que especificó. Este ID, que a veces se denomina *administrador de supervisión*, está diseñado para que lo utilice solo el Centro de operaciones.

No elimine, bloquee o modifique este ID. El mismo ID de administrador con la misma contraseña se registra en los servidores de radio que añade. La contraseña se cambia de forma automática en los servidores concentrador y spoke cada 90 días. No es necesario utilizar ni gestionar dicha contraseña.

Restricción: El Centro de operaciones mantiene el ID de administrador de supervisión y la contraseña en servidores spoke a menos que se utilice una configuración empresarial para gestionar estas credenciales. Para obtener más información acerca de la utilización de una configuración empresarial para gestionar las credenciales, consulte el apartado Consejos para designar la configuración del servidor concentrador y el servidor de radio.

Referencia relacionada:

REGISTER ADMIN (Registrar un ID de administrador)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

IBM Installation Manager

El Centro de operaciones utiliza el IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager todavía no está instalada, se instala de forma automática o se actualiza al instalar Centro de operaciones. Debe permanecer instalada en el sistema para que Centro de operaciones pueda actualizarse o desinstalarse posteriormente según sea necesario.

La siguiente lista contiene explicaciones de algunos de los términos que se utilizan en el gestor de instalación de IBM:

Oferta

Una unidad o producto de software instalable.

La oferta de Centro de operaciones contiene todos los medios que IBM Installation Manager requiere para instalar el Centro de operaciones.

Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de Centro de operaciones contiene los componentes siguientes:

- programa de instalación de IBM Installation Manager
- Oferta de Centro de operaciones

Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

Repositorio


Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de Centro de operaciones se guarda en un repositorio de IBM Fix Central.

Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluyendo archivos que se usan para volver a una versión anterior de Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows






Lista de comprobación de la instalación


Antes de instalar Centro de operaciones, debe verificar cierta información, como las credenciales de instalación y debe determinar la información de entrada que debe proporcionarle a IBM® Installation Manager para la instalación.

La siguiente lista de verificación destaca la información que debe verificar o determinar antes de instalar Centro de operaciones, y Tabla 1 describe los detalles de esta información:




- Verifique el nombre de host del sistema en donde se instalará Centro de operaciones.
- Verifique las credenciales de instalación.
- Determine el directorio de instalación del Centro de operaciones, si no desea aceptar la vía de acceso predeterminada.
- Determine el directorio de instalación de IBM Installation Manager, si no desea aceptar la vía de acceso predeterminada.
- Determine el número de puerto a utilizar por el servidor web Centro de operaciones, si no desea aceptar el número de puerto predeterminado.
- Determine la contraseña para comunicaciones seguras.




Tabla 1. Información para verificar o determinar antes de instalar Centro de operaciones

| Información | Detalles |
|--|--|
| Nombre de host del sistema en el que se instalará Centro de operaciones. | <p>El nombre de host debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> • No debe contener juegos de caracteres de doble bytes (DBCS) o guiones bajos (_). • A pesar de que el nombre de host puede contener el carácter de guión (-), no puede tener un guión como el último carácter del nombre. |
| Credenciales de instalación | <p>Para instalar Centro de operaciones, debe usar la siguiente cuenta de usuario:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX  Sistemas operativos Linux El usuario root •  Sistemas operativos Windows Administrador |
| Directorio de instalación de Centro de operaciones | <p>El Centro de operaciones está instalado en el subdirectorio de instalación de ui.</p> <p>La siguiente vía de acceso es la vía de acceso predeterminada para el directorio de instalación de Centro de operaciones:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX  Sistemas operativos Linux/opt/tivoli/tsm
Por ejemplo, si usa esta vía de acceso predeterminada, Centro de operaciones se instala en el siguiente directorio:

<code>/opt/tivoli/tsm/ui</code> •  Sistemas operativos Windows c:\Program Files\Tivoli\TSM
Por ejemplo, si usa esta vía de acceso predeterminada, Centro de operaciones se instala en el siguiente directorio:

<code>c:\Program Files\Tivoli\TSM\ui</code> <p>La vía de acceso del directorio de instalación debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> • La vía de acceso no debe contener más de 128 caracteres. • La vía de acceso debe incluir solo caracteres ASCII. • La vía de acceso no debe incluir caracteres de control que no se puedan mostrar. • La vía de acceso no debe ninguno de los siguientes caracteres:




<code>% < > ' " \$ & ; *</code> |
| Directorio de instalación de IBM Installation Manager | <p>La siguiente vía de acceso es la vía de acceso predeterminada del directorio de instalación de IBM Installation Manager:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/InstallationManager •  Sistemas operativos Windows C:\Program Files\IBM\Installation Manager |

| Información | Detalles |
|--|---|
| Número de puerto que utiliza el servidor web Centro de operaciones | <p>El valor para el número de puerto seguro (https) debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> • El número debe ser un valor entero entre el rango de 1024 - 65535. • El número no puede estar en uso ni estar asignado a otros programas. <p>Si no especifica un número de puerto, el valor predeterminado es 11090.</p> <p>Consejo: Si posteriormente no recuerda el número de puerto que especificó, consulte el siguiente archivo, donde <i>dir_instalación</i> representa el directorio en donde está instalado Centro de operaciones:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX  Sistemas operativos Linux
<i>dir_instalación/ui/Liberty/usr/servers/guiServer/bootstrap.properties</i> •  Sistemas operativos Windows
<i>dir_instalación\ui\Liberty\usr\servers\guiServer\bootstrap.properties</i> <p>El archivo bootstrap.properties contiene información de conexión del servidor IBM Spectrum Protect.</p> |
| Contraseña para comunicaciones seguras | <p>Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web.</p> <p>El Centro de operaciones requiere una comunicación segura entre el servidor y el Centro de operaciones. Para proteger la comunicación, tiene que añadir el certificado de TLS (seguridad de la capa de transporte) del servidor concentrador al archivo de almacén de confianza del Centro de operaciones.</p> <p>El archivo del almacén de confianza del Centro de operaciones contiene el certificado que el Centro de operaciones utiliza para la comunicación HTTPS con los navegadores web. Durante la instalación de Centro de operaciones, usted crea una contraseña para el archivo del almacén de confianza. Al configurar la comunicación segura entre el Centro de operaciones y el servidor concentrador, debe usar la misma contraseña para agregar el certificado SSL del servidor central al archivo del almacén de confianza.</p> <p>La contraseña del archivo del almacén de confianza debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> • La contraseña debe incluir un mínimo de 6 caracteres y un máximo de 64 caracteres. • La contraseña debe contener como mínimo los siguientes caracteres: <ul style="list-style-type: none"> ◦ Una letra mayúscula (A - Z) ◦ Una letra minúscula (a - z) ◦ Un dígito (de 0 a 9). ◦ Dos de los caracteres no alfanuméricos que se listan en las siguientes series: <pre>~ ! @ # \$ % ^ & * _ - + = ` () { } [] : ; < > , . ? /</pre> |

Tareas relacionadas:

Configuración para la comunicación segura

Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalar el Centro de operaciones




Puede instalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

Antes de empezar

No puede configurar el Centro de operaciones hasta que instale, configure e inicie el servidor de IBM Spectrum Protect. Por lo tanto, antes de instalar Centro de operaciones, instale el paquete de servidor adecuado, de acuerdo con los requisitos de versión del servidor en Requisitos del servidor concentrador y spoke.

Puede instalar el Centro de operaciones en un equipo con el servidor IBM Spectrum Protect o en un sistema independiente.

- Obtención del paquete de instalación de Centro de operaciones
Puede obtener el paquete de instalación de un sitio de descarga de IBM®, como IBM Passport Advantage o IBM Fix Central.
- Instalación de Centro de operaciones utilizando el asistente gráfico
Puede instalar o actualizar Centro de operaciones mediante el asistente gráfico de IBM Installation Manager.
- Instalar el Centro de operaciones en modalidad de consola
Puede instalar o actualizar el Centro de operaciones utilizando la línea de mandatos en la modalidad de consola.
- Instalación de Centro de operaciones en el modo silencioso
Puede instalar o actualizar Centro de operaciones en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Obtención del paquete de instalación de Centro de operaciones

Puede obtener el paquete de instalación de un sitio de descarga de IBM®, como IBM Passport Advantage o IBM Fix Central.

Acerca de esta tarea

Tras obtener el paquete de un sitio de descarga de IBM, debe extraer los archivos de instalación.

Procedimiento

Complete los pasos siguientes para extraer los archivos de instalación de Centro de operaciones. En los pasos siguientes, sustituya *número_versión* con la versión de Centro de operaciones que está instalando.

 Sistemas operativos AIX En los sistemas AIX:

- Descargue el siguiente archivo del paquete al directorio de su elección:

```
número_versión.000
-IBM-SPOC-AIX.bin
```


- Asegúrese de que tiene permisos ejecutables para el archivo del paquete.
Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x número_versión.000-IBM-SPOC-AIX.bin
```

- Emita el siguiente mandato para extraer los archivos de instalación:

```
./número_versión.000-IBM-SPOC-AIX.bin
```

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos Linux En los sistemas Linux:

- Descargue uno de los siguientes archivos del paquete al directorio de su elección:
 - *número_versión.000-IBM-SPOC-LinuxS390.bin*
 - *número_versión.000-IBM-SPOC-Linuxx86_64.bin*
- Asegúrese de que tiene permisos ejecutables para el archivo del paquete.
Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

- Emita el siguiente mandato para extraer los archivos de instalación:



```
./package_name.bin
```

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos Windows En sistemas Windows:


- Descargue el siguiente archivo del paquete al directorio de su elección:
número_versión.000-IBM-SPOC-WindowsX64.exe
- En Windows Explorer, pulse dos veces sobre el nombre del archivo para extraer los archivos de instalación.

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalación de Centro de operaciones utilizando el asistente gráfico

Puede instalar o actualizar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.





 Sistemas operativos AIX

Antes de empezar

Si los siguientes archivos RPM no están instalados en el sistema, instálelos. Para obtener instrucciones, consulte Instalación de archivos RPM para el asistente gráfico.

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm
- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm
- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm

Procedimiento

1. Desde el directorio en el que se extrae el paquete de instalación de Centro de operaciones, emita el siguiente mandato:
 -  Sistemas operativos AIX  Sistemas operativos Linux `./install.sh`
 -  Sistemas operativos Windows `install.bat`
2. Siga las instrucciones del asistente para instalar el IBM Installation Manager y los paquetes de Centro de operaciones.  Sistemas operativos AIX Es posible que se muestre el siguiente mensaje, y que el asistente de instalación funcione de forma lenta si el entorno local utiliza codificación UTF-8:


```
No se puede crear el conjunto de la fuente
```

Si se muestra el mensaje, lleve a cabo una de las siguientes acciones:

- Cambie a un entorno local que no utilice codificación UTF 8. Para los valores de la opción de idiomas que no utilizan codificación UTF 8, consulte Requisitos de idioma.
- Instale el Centro de operaciones mediante la línea de mandatos en la modalidad de consola.
- Instale el Centro de operaciones en modalidad silenciosa.

Qué hacer a continuación

Consulte el apartado Configurar el Centro de Operaciones.



-  Sistemas operativos AIX Instalación de archivos RPM para el asistente gráfico
Antes de poder utilizar el asistente gráfico de IBM Installation Manager para instalar Centro de operaciones, se deben instalar ciertos archivos RPM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows


Instalar el Centro de operaciones en modalidad de consola

Puede instalar o actualizar el Centro de operaciones utilizando la línea de mandatos en la modalidad de consola.

Procedimiento

1. En el directorio en el que se extrae el archivo del paquete de instalación, ejecute el siguiente mandato:
 Sistemas operativos AIX  Sistemas operativos Linux

```
./install.sh -c
```




 Sistemas operativos Windows

```
install.bat -c
```

2. Siga las instrucciones de la consola para instalar Installation Manager y los paquetes de Centro de operaciones.

Qué hacer a continuación

Consulte el apartado Configurar el Centro de Operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalación de Centro de operaciones en el modo silencioso

Puede instalar o actualizar Centro de operaciones en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

Antes de empezar

Para proporcionar entrada de datos cuando utilice el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install_response_sample.xml

Utilice este archivo para instalar Centro de operaciones.

update_response_sample.xml

Utilice este archivo para actualizar Centro de operaciones.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

Procedimiento

1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
Consejo: Para generar un archivo de respuesta como parte de la instalación, efectúe la selección de las opciones de instalación de la modalidad de consola. A continuación en el panel Resumen, escriba G para generar el archivo de respuesta según las opciones seleccionadas anteriormente.
2. Cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.
Si está utilizando el archivo install_response_sample.xml, añada la contraseña en la línea siguiente del archivo, donde *mypassword* representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de la instalación.

Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo update_response_sample.xml.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor *archivo_respuestas* representa la vía de acceso del archivo de respuestas y el nombre del archivo:

-  Sistemas operativos AIX  Sistemas operativos Linux

```
./install.sh -s -input archivo_respuestas -acceptLicense
```

-  Sistemas operativos Windows

```
install.bat -s -input archivo_respuestas -acceptLicense
```

Qué hacer a continuación

Consulte el apartado Configurar el Centro de Operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Actualización del Centro de operaciones

Puede actualizar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.



Antes de empezar

Antes de actualizar el Centro de operaciones, revise los requisitos de sistema y la lista de comprobación de instalación. La nueva versión del Centro de operaciones puede tener requisitos y consideraciones adicionales o diferentes de los de la versión que se está utilizando actualmente.

Acerca de esta tarea

Las instrucciones para actualizar Centro de operaciones son las mismas que las instrucciones para instalar Centro de operaciones, con las siguientes excepciones:

- Puede usar la función Actualizar de IBM® Installation Manager en vez de la función Instalar.
Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.
- Si está actualizando Centro de operaciones en el modo silencioso, puede omitir el paso de crear una contraseña para el archivo del almacén de confianza.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Guía de inicio de la Centro de operaciones

Antes de poder utilizar Centro de operaciones para gestionar el entorno de almacenamiento, debe configurarlo.

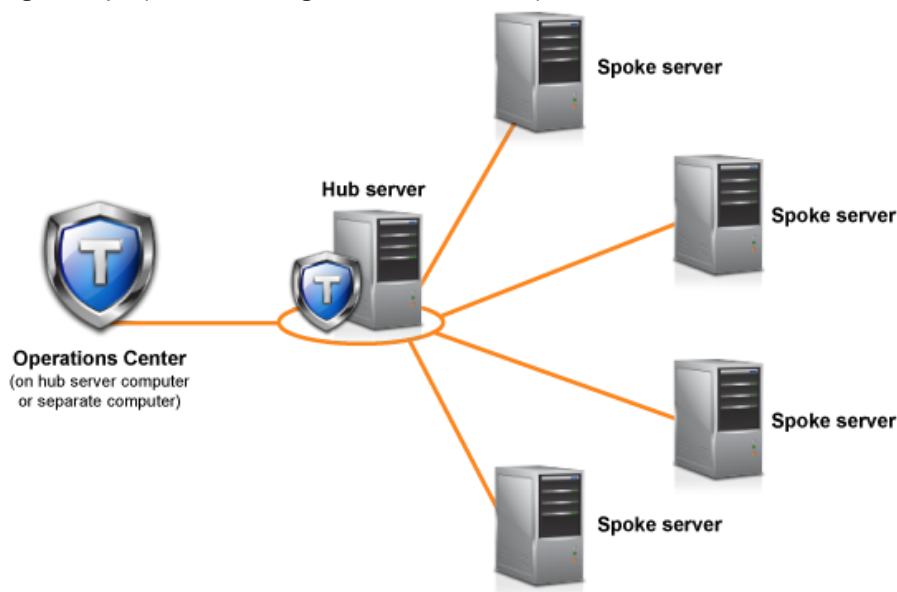
Acerca de esta tarea

Después de instalar el Centro de operaciones, realice los pasos de configuración básicos siguientes:

1. Designe el servidor concentrador.
2. Añada los servidores de radio.
3. Si lo desea, configure alertas de correo electrónico en los servidores concentrador y de radio.




Figura 1 ilustra una configuración del Centro de operaciones.

Figura 1. Ejemplo de una configuración de Centro de operaciones con los servidores concentrador y de radio



- Configurar el Centro de Operaciones
Al abrir Centro de operaciones por primera vez, debe configurarlo para gestionar el entorno de almacenamiento. Debe asociar Centro de operaciones con el servidor IBM Spectrum Protect que se ha designado como el servidor concentrador. A continuación puede conectar servidores IBM Spectrum Protect adicionales como servidores de radio.



- Configuración para la comunicación segura
Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web. El protocolo TLS (seguridad de la capa de transporte) protege las comunicaciones entre el centro de operaciones y el servidor concentrador, y entre el servidor concentrador y los servidores spoke asociados.
- Iniciar y detener el servidor web
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Apertura del Centro de operaciones
La página Visión general es la vista inicial predeterminada del Centro de operaciones. Sin embargo, en el navegador web, puede marcar la página que desea que se abra cuando inicie la sesión en el Centro de operaciones.
- Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect
El servicio de gestión de clientes recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y hace que la información esté disponible para el Centro de operaciones para la prestación de supervisión básica.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Configurar el Centro de Operaciones

Al abrir Centro de operaciones por primera vez, debe configurarlo para gestionar el entorno de almacenamiento. Debe asociar Centro de operaciones con el servidor IBM Spectrum Protect que se ha designado como el servidor concentrador. A continuación puede conectar servidores IBM Spectrum Protect adicionales como servidores de radio.

- Designar el servidor central
Cuando se conecta a Centro de operaciones por primera vez, debe designar qué servidor IBM Spectrum Protect es el servidor central.
- Adición de un servidor de radio
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Envío de alertas por correo electrónico a los administradores
Una alerta es una notificación de un problema importante en el servidor IBM Spectrum Protect y se desencadena mediante un mensaje de servidor. Las alertas se muestran en Centro de operaciones y se pueden enviar desde el servidor a los administradores por correo electrónico.
- Adición de texto personalizado a la pantalla de inicio de sesión
Puede añadir texto personalizado, por ejemplo los términos de uso del software de la organización, a la pantalla de inicio de sesión del Centro de operaciones de modo que los usuarios del Centro de operaciones vean el texto antes de que entren el nombre de usuario y la contraseña.
- Habilitación de servicios REST
Las aplicaciones que utilizan servicios REST (Representational State Transfer) pueden consultar y gestionar el entorno de almacenamiento conectándose al Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Designar el servidor central

Cuando se conecta a Centro de operaciones por primera vez, debe designar qué servidor IBM Spectrum Protect es el servidor central.

Antes de empezar

El Centro de operaciones requiere la comunicación segura entre el servidor concentrador y el Centro de operaciones. Para proteger la comunicación, tiene que añadir el certificado de TLS (seguridad de la capa de transporte) del servidor concentrador al archivo de almacén de confianza del Centro de operaciones. Para obtener más información, consulte el apartado Protección de la comunicación entre el centro de operaciones y el servidor concentrador.

Procedimiento

En un navegador web, escriba la siguiente dirección, en donde *hostname* representa el nombre del sistema en donde está instalado Centro de operaciones *secure_port*, y representa el número de puerto que utiliza Centro de operaciones para la comunicación HTTPS en ese sistema:

```
https://nombrehost:puerto_seguro/oc
```

Consejos:

- El URL es sensible a las mayúsculas y minúsculas. Por ejemplo, asegúrese de que escribe "oc" en minúsculas como se indica.

- Para obtener más información sobre el número de puerto, consulte la Lista de comprobación de instalación.
- Si se está conectando al Centro de operaciones por primera vez, debe proporcionar la siguiente información:
 - La información de conexión para el servidor que desea designar como servidor concentrador.
 - Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor
- Si el periodo de retención del registro de sucesos es inferior al de 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor concentrador.

Qué hacer a continuación




Si tiene varios servidores IBM Spectrum Protect en el entorno, añada los otros servidores como servidores de radio al servidor concentrador.

Atención: No cambie el nombre de un servidor, después de que se haya configurado como servidor de radio o servidor concentrador.

Conceptos relacionados:

Requisitos del servidor concentrador y spoke

Los ID de administrador que requiere el centro de operaciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Adición de un servidor de radio

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

Antes de empezar

La comunicación entre el servidor spoke y el servidor concentrador debe protegerse utilizando el protocolo TLS (Seguridad de la capa de transporte). Para proteger la comunicación, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

Procedimiento




1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
 - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
 - Si el servidor que quiere añadir no aparece en la tabla y no es necesaria la comunicación SSL/TLS segura, pulse + Spoke en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor de radio.

Referencia relacionada:

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Envío de alertas por correo electrónico a los administradores

Una alerta es una notificación de un problema importante en el servidor IBM Spectrum Protect y se desencadena mediante un mensaje de servidor. Las alertas se muestran en Centro de operaciones y se pueden enviar desde el servidor a los administradores por correo electrónico.

Antes de empezar

Para poder configurar la notificación por correo electrónico para los administradores sobre las alertas, asegúrese de que se cumplan los requisitos siguientes:

- Es necesario un servidor SMTP para enviar y recibir alertas por correo electrónico, y el servidor que envía las alertas por correo electrónico debe tener acceso al servidor SMTP.

Consejo: Si Centro de operaciones está instalado en un sistema independiente, dicho sistema no necesita acceder al servidor SMTP.

- Un administrador debe tener privilegio de sistema para poder configurar la notificación por correo electrónico.

Acerca de esta tarea

Solo se envía una notificación de correo electrónico para la primera aparición de una alerta. Además, si se genera una alerta antes de configurar la notificación de correo electrónico, no se enviará ninguna notificación de correo electrónico para dicha alerta.

Puede configurar la notificación por correo electrónico de las maneras siguientes:

- Enviar notificación para alertas individuales
- Enviar resúmenes de alertas

Un resumen de alerta contiene información sobre las alertas actuales. El resumen incluye el número total de alertas, el número total de alertas activas e inactivas, la alerta más antigua, la alerta más reciente y la alerta que se produce con más frecuencia.

Puede especificar hasta tres administradores para recibir resúmenes de alertas por correo electrónico. Los resúmenes de alertas se envían, aproximadamente, cada hora.

Procedimiento

Para configurar las notificaciones de correo electrónico para los administradores sobre las alertas, realice los pasos siguientes en cada servidor rápido y concentrador del que desee recibir alertas de correo electrónico:

1. Para verificar que la supervisión de alertas está activada, emita el mandato siguiente:

```
QUERY MONITORSETTINGS
```

2. Si la salida del mandato indica que la supervisión de alertas está desactivada, emita el mandato siguiente. De lo contrario, continúe con el paso siguiente.

```
SET ALERTMONITOR ON
```

3. Para habilitar el envío de notificaciones por correo electrónico, emita el mandato siguiente:

```
SET ALERTEMAIL ON
```

4. Para definir el servidor SMTP que se utilizará para enviar las notificaciones por correo electrónico, emita el mandato siguiente:

```
SET ALERTEMAILSMTPHOST nombre_host
```

5. Para especificar el número de puerto para el servidor SMTP, emita el mandato siguiente:

```
SET ALERTEMAILSMTPPORT número_puerto
```

El número de puerto predeterminado es 25.

6. Para especificar la dirección de correo electrónico del remitente de las alertas, emita el mandato siguiente:

```
SET ALERTEMAILFROMADDR dirección_correo_electrónico
```

7. Para cada ID de administrador que debe recibir una notificación por correo electrónico, emita uno de los mandatos siguientes para activar la notificación de correo electrónico y especificar la dirección de correo electrónico:

```
REGISTER ADMIN nombre_admin ALERT=YES EMAILADDRESS=dirección_correo_electrónico
```

```
UPDATE ADMIN nombre_admin ALERT=YES EMAILADDRESS=dirección_correo_electrónico
```

8. Elija una de las dos opciones siguientes, o ambas, y especifique el ID de administrador para recibir una notificación por correo electrónico:

- Enviar notificación para alertas individuales

Para especificar o actualizar los ID de administrador para recibir una notificación por correo electrónico para una alerta individual, emita uno de los mandatos siguientes:

```
DEFINE ALERTTRIGGER número_mensaje Admin=nombre_admin1, nombre_admin2
```

```
UPDATE ALERTTRIGGER número_mensaje ADDadmin=nombre_admin3 DELadmin=nombre_admin1
```

Consejo: En la página Configurar alertas del Centro de operaciones, puede seleccionar los administradores que recibirán la notificación de correo electrónico.

- Enviar resúmenes de alertas

Para especificar o actualizar los ID de administrador para recibir resúmenes de alertas por correo electrónico, emita el mandato siguiente:

```
SET ALERTSUMMARYTOADMINS nombre_admin1, nombre_admin2, nombre_admin3
```

Si desea recibir resúmenes de alertas, pero no desea recibir notificaciones sobre alertas individuales, realice los pasos siguientes:

- Suspenda la notificación sobre alertas individuales, tal como se describe en Suspensión temporal de alertas por correo electrónico.
- Asegúrese de que el ID de administrador correspondiente figure en el mandato siguiente:

```
SET ALERTSUMMARYTOADMINS nombre_admin1, nombre_admin2, nombre_admin3
```

Envío de alertas por correo electrónico a varios administradores

El ejemplo siguiente muestra los mandatos que hacen que las alertas para el mensaje ANR1075E se envíen en un correo electrónico a los administradores myadmin, djadmin y csadmin:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

- Suspensión temporal de alertas por correo electrónico
En determinadas situaciones, es posible que desee suspender las alertas de correo electrónico de forma temporal. Por ejemplo, es posible que desee recibir resúmenes de alertas pero no suspender las notificaciones sobre alertas individuales, o es posible que desee suspender las alertas por correo electrónico cuando un administrador esté de vacaciones.

Referencia relacionada:

DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)

QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)

REGISTER ADMIN (Registrar un ID de administrador)

SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)

SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)

SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)


SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)

SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)

SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)

UPDATE ADMIN (Actualizar un administrador)

UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Adición de texto personalizado a la pantalla de inicio de sesión

Puede añadir texto personalizado, por ejemplo los términos de uso del software de la organización, a la pantalla de inicio de sesión del Centro de operaciones de modo que los usuarios del Centro de operaciones vean el texto antes de que entren el nombre de usuario y la contraseña.

Procedimiento

Para añadir texto personalizado a la pantalla de inicio de sesión, realice los pasos siguientes:

- En el sistema donde está instalado Centro de operaciones, vaya al directorio siguiente, donde *dir_instalación* representa el directorio en el cual está instalado Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación*/ui/Liberty/usr/servers/guiServer

 Sistemas operativos Windows *dir_instalación*\ui\Liberty\usr\servers\guiServer

- En el directorio, cree un archivo denominado loginText.html que contiene el texto que desea añadir a la pantalla de inicio de sesión. Cualquier texto especial que no sea ASCII debe estar codificado en UTF-8.
Consejo: Puede formatear el texto añadiendo las etiquetas HTML.
- Revise el texto añadido en la pantalla de inicio de sesión del Centro de operaciones.

Para abrir el Centro de operaciones, entre la siguiente dirección en un navegador web, donde *nombrehost* representa el nombre del sistema donde está instalado el Centro de operaciones y *puerto_seguro* representa el número de puerto que el Centro de operaciones utiliza para la comunicación HTTPS en ese sistema:

```
https://nombrehost:puerto_seguro/oc
```

Habilitación de servicios REST

Las aplicaciones que utilizan servicios REST (Representational State Transfer) pueden consultar y gestionar el entorno de almacenamiento conectándose al Centro de operaciones.

Acerca de esta tarea

Habilite esta característica para permitir que los servicios REST interactúen con los servidores concentrador y de radio enviando llamadas a la siguiente dirección:


```
https://nombre_host_co:puerto/oc/api
```




donde *nombre_host_co* es el nombre de red o la dirección IP del sistema host del Centro de operaciones y *puerto* es el número de puerto del Centro de operaciones. El número de puerto predeterminado es 11090.

Para obtener información sobre los servicios REST que están disponibles para el Centro de operaciones, consulte la nota técnica <http://www.ibm.com/support/docview.wss?uid=swg21973011> o emita la siguiente llamada REST:

```
https://nombre_host_co:puerto/oc/api/help
```

Procedimiento

1. En la barra de menús del Centro de operaciones, pase el cursor por encima del icono de configuración  y pulse Configuración.
2. En la página General, marque el recuadro de selección Habilitar API de REST administrativa.
3. Pulse Guardar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




Configuración para la comunicación segura

Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web. El protocolo TLS (seguridad de la capa de transporte) protege las comunicaciones entre el centro de operaciones y el servidor concentrador, y entre el servidor concentrador y los servidores spoke asociados.

Acerca de esta tarea

Se requiere TLS 1.2 para la comunicación segura entre el servidor IBM Spectrum Protect y el Centro de operaciones, y entre el servidor concentrador y los servidores spoke.

- Protección de la comunicación entre el centro de operaciones y el servidor concentrador
Para proteger las comunicaciones entre el Centro de operaciones y el servidor concentrador, debe añadir el certificado TLS (seguridad de la capa de transporte) a un archivo de almacén de confianza del Centro de operaciones.
- Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke
Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke mediante el protocolo de capa de sockets seguros (TLS), es necesario definir el certificado del servidor spoke en el servidor concentrador, y el certificado del servidor concentrador en el servidor spoke. También debe configurar Centro de operaciones para supervisar el servidor de radio.
- Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones
Para configurar la comunicación segura entre Centro de operaciones y el servidor central, debe conocer la contraseña del archivo del almacén de confianza de Centro de operaciones. Se crea esta contraseña durante la instalación de Centro de operaciones. Si no conoce la contraseña, puede restaurarla.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Protección de la comunicación entre el centro de operaciones y el servidor concentrador

Para proteger las comunicaciones entre el Centro de operaciones y el servidor concentrador, debe añadir el certificado TLS (seguridad de la capa de transporte) a un archivo de almacén de confianza del Centro de operaciones.

Antes de empezar

El archivo de almacén de confianza del Centro de operaciones es un contenedor para certificados al que puede acceder Centro de operaciones. El archivo del almacén de confianza contiene el certificado que Centro de operaciones usa para la comunicación HTTPS con los navegadores web.

Durante la instalación de Centro de operaciones, cree una contraseña para el archivo del almacén de confianza. Para proteger la comunicación entre el Centro de operaciones y el servidor concentrador, debe usar la misma contraseña para agregar el certificado SSL del servidor central al archivo del almacén de confianza. Si no recuerda la contraseña, puede restaurarla. Consulte el apartado Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones.

Procedimiento

1. Especifique el certificado cert256.arm como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador.

Para especificar cert256.arm como el certificado predeterminado, siga los pasos a continuación:

- a. Emita el siguiente mandato desde el directorio de la instancia del servidor central:

```
gsk8capiCmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```



- b. Reinicie el servidor central de manera que pueda recibir los cambios en el archivo de la base de datos clave.


2. Para verificar que el certificado cert256.arm está establecido como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador, emita el siguiente mandato:

```
gsk8capiCmd_64 -cert -list -db cert.kdb -stashed
```

3. Detenga el servidor web de Centro de operaciones.
4. Vaya a la línea de mandatos del sistema operativo en el cual está instalado Centro de operaciones.
5. Añada el certificado al archivo de almacén de confianza de Centro de operaciones utilizando el programa de utilidad iKeycmd o el programa de utilidad iKeyman.




El programa de utilidad iKeycmd es una interfaz de línea de mandatos y el programa de utilidad iKeyman es la interfaz gráfica de usuario de IBM® Key Management.

 Sistemas operativos AIX  Sistemas operativos Linux Los programas de utilidad iKeycmd y iKeyman se deben ejecutar como usuario root.

 Sistemas operativos Windows Los programas de utilidad iKeycmd y iKeyman se deben ejecutar con una cuenta de administrador.

Para añadir el certificado TLS utilizando la interfaz de línea de mandatos, realice los pasos siguientes:

- a. Vaya al directorio siguiente, donde *dir_instalación* representa el directorio en el cual está instalado Centro de operaciones:

-  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación/ui/jre/bin*
-  Sistemas operativos Windows *dir_instalación\ui\jre\bin*

- b. Emita el mandato iKeycmd para añadir el certificado cert256.arm como certificado predeterminado en el archivo de base de datos de claves del servidor concentrador:

```
ikeycmd -cert -add  
-db /dir_instalación/Liberty/usr/servers/guiServer/gui-truststore.jks  
-file /fvt/comfrey/srv/cert256.arm  
-label 'descripción etiqueta'  
-pw 'contraseña' -type jks -format ascii -trust enable
```

donde:

dir_instalación

El directorio en el cual está instalado Centro de operaciones.

descripción etiqueta




Descripción que asigna a la etiqueta.

contraseña

La contraseña que ha creado al instalar Centro de operaciones. Para restablecer la contraseña, desinstale Centro de operaciones, suprima el archivo .jks y vuelva a instalar Centro de operaciones.

Para añadir el certificado utilizando la ventana IBM Key Management, realice los pasos siguientes:

a. Vaya al directorio siguiente, donde *dir_instalación* representa el directorio en el cual está instalado Centro de operaciones:




-  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación/ui/jre/bin*
-  Sistemas operativos Windows *dir_instalación\ui\jre\bin*

b. Abra la ventana IBM Key Management emitiendo el siguiente mandato:

```
ikeyman
```

c. Pulse Archivo de base de datos de claves > Abrir.

d. En la ventana Open, pulse Browse, y vaya al siguiente directorio, en donde *dir_instalación* representa el directorio en el cual está instalado el Centro de operaciones:

-  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación/ui/Liberty/usr/servers/guiServer*
-  Sistemas operativos Windows *dir_instalación\ui\Liberty\usr\servers\guiServer*

e. En el directorio guiServer, seleccione el archivo gui-truststore.jks.




f. Pulse Abrir, y pulse Aceptar.

g. Especifique la contraseña del archivo de almacén de confianza y pulse Aceptar.

h. En el área Contenido de la base de datos clave de la ventana Gestión de claves de IBM, pulse la flecha y seleccione Certificados del signatario de la lista.

i. Pulse Añadir.




j. En la ventana Abrir, pulse Examinar, y vaya al directorio de la instancia del servidor central que se muestra en el siguiente ejemplo:

-  Sistemas operativos AIX  Sistemas operativos Linux *opt/tivoli/tsm/server/bin*
-  Sistemas operativos Windows *c:\Program Files\Tivoli\TSM\server1*

El directorio contiene el certificado cert256.arm.

Si no puede acceder al directorio de la instancia del servidor central desde la ventana Open, complete los siguientes pasos:

i. Utilice FTP u otro método de transferencia de archivos para copiar los archivos de cert256.arm en el servidor concentrador en el siguiente directorio del sistema donde se ha instalado el Centro de operaciones:

-  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación/ui/Liberty/usr/servers/guiServer*
-  Sistemas operativos Windows *dir_instalación\ui\Liberty\usr\servers\guiServer*

ii. En la ventana Open, vaya al directorio guiServer.

k. Seleccione el certificado cert256.arm como certificado.

Consejo: El certificado que elija debe establecerse como certificado predeterminado en el archivo de base de datos de claves del servidor concentrador. Para obtener más información, consulte el paso 1 y 2.

l. Pulse Abrir, y pulse Aceptar.

m. Escriba una etiqueta para el certificado. Por ejemplo, escriba el nombre del servidor central.




n. Pulse Aceptar. El certificado SSL del servidor central se añade al archivo del almacén de confianza, y se muestra la etiqueta en el área Contenido de la base de datos clave de la ventana Gestión de claves de IBM.

o. Cierre la ventana IBM Key Management.

6. Inicie el servidor web del Centro de operaciones.

7. Al conectarse al Centro de operaciones por primera vez, se le solicita que identifique la dirección IP o el nombre de red del servidor concentrador, y el número de puerto para comunicarse con el servidor concentrador. Si la opción de servidor ADMINONCLIENTPORT está habilitada para el servidor IBM Spectrum Protect, especifique el número de puerto especificado por la opción de servidor TCPADMINPORT. Si la opción de servidor ADMINONCLIENTPORT no está habilitada, especifique el número de puerto especificado por la opción de servidor TCPSPORT.

Si Centro de operaciones se ha configurado previamente, puede revisar el contenido del archivo serverConnection.properties para verificar la información de conexión. El archivo serverConnection.properties se encuentra en el directorio siguiente en el sistema donde está instalado Centro de operaciones:




- o  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación/ui/Liberty/usr/servers/guiServer*
- o  Sistemas operativos Windows *dir_instalación\ui\Liberty\usr\servers\guiServer*

Qué hacer a continuación

Para establecer la comunicación TLS entre el servidor concentrador y un servidor de radio, consulte Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke.

Referencia relacionada:

QUERY OPTION (Consultar opciones del servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke

Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke mediante el protocolo de capa de sockets seguros (TLS), es necesario definir el certificado del servidor spoke en el servidor concentrador, y el certificado del servidor concentrador en el servidor spoke. También debe configurar Centro de operaciones para supervisar el servidor de radio.

Acerca de esta tarea

El servidor concentrador recibe información de alerta y estado del servidor de radio y muestra esta información en el Centro de operaciones. Para recibir información de estado y de alerta del servidor de radio, debe añadirse el certificado del servidor de radio al archivo de almacén de confianza del servidor concentrador. También debe configurar Centro de operaciones para supervisar el servidor de radio.

Para habilitar otras funciones del Centro de operaciones, como el despliegue automático de actualizaciones del cliente, el certificado del servidor concentrador debe añadirse al archivo de almacén de confianza del servidor de radio.

Procedimiento

1. Realice los pasos siguientes para definir el certificado del servidor de radio en el servidor concentrador:

- a. En el servidor de radio, cambie al directorio de la instancia del servidor de radio.
- b. Especifique el certificado `cert256.arm` necesario como el certificado predeterminado en el archivo de base de datos de claves del servidor de radio. Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

- c. Verifique los certificados que hay en el archivo de base de datos de claves del servidor de radio: Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -list -db cert.kdb -stashed
```

- d. Transfiera de forma el archivo `cert256.arm` del servidor de radio al servidor central.
- e. En el servidor central, cambie el directorio de la instancia del servidor central.
- f. Defina el certificado del servidor de radio en el servidor concentrador. Emita el siguiente mandato desde el directorio de la instancia del servidor concentrador, donde `nombre_servidor_spoke` es el nombre del servidor de radio y `spoke_cert256.arm` es el nombre de archivo del certificado del servidor de radio:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label spoke_servername -file spoke_cert256.arm
```

2. Realice los pasos siguientes para definir el certificado del servidor concentrador en el servidor de radio:

- a. En el servidor central, cambie el directorio de la instancia del servidor central.
- b. Especifique el certificado `cert256.arm` necesario como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador. Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

- c. Verifique los certificados que hay en el archivo de base de datos de claves del servidor de radio: Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -list -db cert.kdb -stashed
```

- d. Transfiera de forma el archivo `cert256.arm` del servidor concentrador al servidor de radio.
- e. En el servidor de radio, cambie al directorio de la instancia del servidor de radio.
- f. Defina el certificado del servidor concentrador en el servidor de radio. Emita el siguiente mandato desde el directorio de la instancia del servidor de radio, donde `nombre_servidor_concentrador` es el nombre del servidor concentrador y `hub_cert256.arm` es el nombre de archivo del certificado del servidor concentrador:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label nombre_servidor_concentrador -file hub_cert256.arm
```

3. Reinicie el servidor central y el servidor de radio.

4. Realice los pasos siguientes para definir el servidor de radio para el servidor concentrador, y el servidor concentrador para el servidor de radio.

- a. Emita los mandatos siguientes tanto en el servidor concentrador como en el servidor de radio:

```
SET SERVERPASSWORD contraseña_servidor  
SET SERVERHLADDRESS dirección_ip  
SET SERVERLLADDRESS puerto_tcp
```

- b. En el servidor concentrador, emita el mandato `DEFINE SERVER`, de acuerdo con el ejemplo siguiente:

```
DEFINE SERVER spoke_servername HLA=spoke_address
LLA=spoke_SSLTCPADMINPort SERVERPA=spoke_serverpassword
```

c. En el servidor de radio, emita el mandato DEFINE SERVER, de acuerdo con el ejemplo siguiente:

```
DEFINE SERVER nombre_servidor_concentrador HLA=dirección_concentrador
LLA=hub_SSLTCPADMINPort SERVERPA=contraseña_servidor_concentrador
```




Consejo: De forma predeterminada, la comunicación del servidor está cifrada excepto cuando el servidor envía o recibe datos de objeto. Los datos de objeto se envían y reciben mediante el protocolo TCP/IP. Si elige no cifrar los datos de objeto, el rendimiento del servidor será similar a la comunicación sobre una sesión TCP/IP y la sesión es segura. Para cifrar toda la comunicación con el servidor especificado, incluso cuando el servidor envía y recibe datos de objeto, especifique el parámetro SSL=YES en el mandato DEFINE SERVER.

5. Realice los pasos siguientes para configurar el Centro de operaciones para supervisar el servidor de radio:
 - a. En la barra de menús de Centro de operaciones, pulse Servidores. El servidor de radio tiene el estado "No supervisado". Este estado significa que, aunque se haya definido este servidor en el servidor concentrador utilizando el mandato DEFINE SERVER, el servidor aún no está configurado como servidor de radio.
 - b. Pulse el servidor de radio (spoke) para resaltar el elemento y pulse Supervisar radio.

Referencia relacionada:

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

QUERY OPTION (Consultar opciones del servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones

Para configurar la comunicación segura entre Centro de operaciones y el servidor central, debe conocer la contraseña del archivo del almacén de confianza de Centro de operaciones. Se crea esta contraseña durante la instalación de Centro de operaciones. Si no conoce la contraseña, puede restaurarla.

Acerca de esta tarea

Para restablecer la contraseña, debe crear una nueva contraseña, eliminar el archivo del almacén de confianza de Centro de operaciones, y reiniciar el servidor web Centro de operaciones.

Procedimiento

1. Detenga el servidor web de Centro de operaciones.
2. Vaya al directorio siguiente, donde *dir_instalación* representa el directorio en el cual está instalado Centro de operaciones:
 - o  Sistemas operativos AIX  Sistemas operativos Linux *dir_instalación*/ui/Liberty/usr/servers/guiServer
 - o  Sistemas operativos Windows *dir_instalación*\ui\Liberty\usr\servers\guiServer
3. Abra el archivo bootstrap.properties, que contiene la contraseña del archivo del almacén de confianza. Si la contraseña no está cifrada, puede usarla para abrir el archivo del almacén de confianza sin tener que restablecerla.

El siguiente ejemplo indica la diferencia entre una contraseña cifrada y una no cifrada:

Ejemplo de una contraseña cifrada

Las contraseñas cifradas comienzan con la cadena de texto {xor}.

El siguiente ejemplo muestra la contraseña cifrada como el valor del parámetro tsm.truststore.pswd:

```
tsm.truststore.pswd={xor}MiYPPiwsKDAtoW==
```

Ejemplo de contraseña no cifrada

El siguiente ejemplo muestra la contraseña no cifrada como el valor del parámetro tsm.truststore.pswd:

```
tsm.truststore.pswd=J8b%^B
```

4. Reinicie la contraseña sustituyéndola en el archivo bootstrap.properties por la contraseña nueva. Puede sustituir la contraseña con una contraseña cifrada o no cifrada. Recuerde la contraseña no cifrada para uso en el futuro.

Para crear una contraseña encriptada, siga estos pasos:

- a. Cree una contraseña sin cifrar.

La contraseña del archivo del almacén de confianza debe cumplir con los siguientes criterios:

- La contraseña debe incluir un mínimo de 6 caracteres y un máximo de 64 caracteres.
- La contraseña debe contener como mínimo los siguientes caracteres:
 - Una letra mayúscula (A - Z)
 - Una letra minúscula (a - z)

- Un dígito (de 0 a 9).
- Dos de los caracteres no alfanuméricos que se listan en las siguientes series:

```
~ ! @ # $ % ^ & * _ - + = ` |
( ) { } [ ] : ; < > , . ? /
```

b. Desde la línea de mandatos del sistema operativo, vaya al siguiente directorio:

- Sistemas operativos AIX Sistemas operativos Linux `dir_instalación/ui/Liberty/bin`
- Sistemas operativos Windows `dir_instalación\ui\Liberty\bin`

c. Para cifrar la contraseña, emita el siguiente mandato, en donde *myPassword* representa la contraseña cifrada:

- Sistemas operativos AIX Sistemas operativos Linux `securityUtility encode myPassword`
- Sistemas operativos Windows `securityUtility.bat encode myPassword`

Sistemas operativos Windows Podría aparecer el mensaje siguiente:

```
! "java" is not recognized as an internal or external command,
programa operativo o archivo por lotes.
```

Si se muestra este mensaje, siga estos pasos:

- i. Emita el siguiente mandato, en donde *dir_instalación* representa el directorio en donde está instalado Centro de operaciones:

```
set JAVA_HOME="dir_instalación\ui\jre"
```

- ii. Vuelva a emitir el siguiente mandato para cifrar la contraseña:

```
securityUtility.bat encode myPassword
```

5. Cierre el archivo `bootstrap.properties`.

6. Vaya al directorio siguiente:

- o Sistemas operativos AIX Sistemas operativos Linux `dir_instalación/ui/Liberty/usr/servers/guiServer`
- o Sistemas operativos Windows `dir_instalación\ui\Liberty\usr\servers\guiServer`

7. Elimine el archivo `gui-truststore.jks`, que es el archivo del almacén de confianza de Centro de operaciones.

8. Inicie el servidor web Centro de operaciones.

Resultados

Se crea automáticamente un nuevo archivo del almacén de confianza para Centro de operaciones, y el certificado TLS de Centro de operaciones se incluye de manera automática en el archivo del almacén de confianza.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows

Iniciar y detener el servidor web

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.

Procedimiento

Detenga e inicie el servidor web.

- Sistemas operativos AIX Desde el directorio `/dir_instalación/ui/utls`, donde *dir_instalación* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

- o Para detener el servidor:

```
./stopserver.sh
```

- o Para iniciar el servidor:

```
./startserver.sh
```

- Sistemas operativos Linux Emita los mandatos siguientes:

- o Para detener el servidor:

```
service opscenter.rc stop
```

- o Para iniciar el servidor:


```
service opscenter.rc start
```


- Para reiniciar el servidor:

```
service opscenter.rc restart
```

Para determinar si el servidor está ejecutándose, emita el siguiente mandato:

```
service opscenter.rc status
```

-  Sistemas operativos Windows Desde la ventana Servicios, detenga o inicie el servicio Centro de operaciones.

Apertura del Centro de operaciones

La página Visión general es la vista inicial predeterminada del Centro de operaciones. Sin embargo, en el navegador web, puede marcar la página que desea que se abra cuando inicie la sesión en el Centro de operaciones.

Procedimiento

1. En un navegador web, escriba la siguiente dirección, en donde *hostname* representa el nombre del sistema en donde está instalado Centro de operaciones *secure_port*, y representa el número de puerto que utiliza Centro de operaciones para la comunicación HTTPS en ese sistema:


```
https://nombrehost:puerto_seguro/oc
```

Consejos:

- El URL es sensible a las mayúsculas y minúsculas. Por ejemplo, asegúrese de que escribe "oc" en minúsculas como se indica.
 - El número de puerto predeterminado para la comunicación HTTPS es 11090, pero se puede especificar un número de puerto diferente durante la instalación de Centro de operaciones.
2. Inicie la sesión, utilizando un ID de administrador registrado en el servidor concentrador.

En la página Visión general, puede ver información de resumen para clientes, servicios, servidores, agrupaciones de almacenamiento y dispositivos de almacenamiento. Puede ver más detalles pulsando elementos o utilizando la barra de menú del Centro de operaciones.

Supervisión desde un dispositivo móvil: Para supervisar de forma remota el entorno de almacenamiento, puede ver la página Visión general del Centro de operaciones en el navegador web de un dispositivo móvil. El Centro de operaciones soporta el navegador web Safari de Apple en el iPad. También se pueden utilizar otros dispositivos móviles.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect

El servicio de gestión de clientes recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y hace que la información esté disponible para el Centro de operaciones para la prestación de supervisión básica.

Acerca de esta tarea

Después de instalar el servicio de gestión de clientes, puede ver la página Diagnóstico en el Centro de operaciones para obtener información de resolución de problemas para los clientes de archivado y copia de seguridad.


La información de diagnóstico se puede recopilar solo desde clientes Linux y Windows. pero los administradores pueden ver la información de diagnóstico en Centro de operaciones en sistemas operativos AIX, Linux o Windows.

También puede instalar el servicio de gestión de clientes en nodos de transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware para recopilar información de diagnóstico sobre los transportadores de datos.

Consejo: En la documentación de servicio de gestión de clientes, *sistema cliente* es el sistema donde está instalado el cliente de archivado y copia de seguridad.

- Instalación de servicio de gestión de clientes utilizando el asistente gráfico
Para recopilar información de diagnóstico sobre los clientes de archivado y copia de seguridad, por ejemplo archivos de registro de cliente, debe instalar el servicio de gestión de clientes en los sistemas cliente que gestiona.
- Instalación de servicio de gestión de clientes en modalidad silenciosa
Puede instalar el servicio de gestión de clientes en modalidad silenciosa. Cuando se utiliza la modalidad silenciosa, se

- proporcionan los valores de instalación en un archivo de respuestas y, a continuación, se ejecuta un mandato de instalación.
- Verificación de que el servicio de gestión de clientes está instalado correctamente
Antes de utilizar el servicio de gestión de clientes para recopilar información de diagnóstico acerca de un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de clientes esté instalado y configurado correctamente.
- Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes
Si no ha utilizado la configuración predeterminada para el servicio de gestión de clientes, debe configurar el Centro de operaciones para acceder al servicio de gestión de clientes.
- Inicio y detención del servicio de gestión de clientes
El servicio de gestión de clientes se inicia automáticamente después de instalarse en el sistema cliente. Es posible que necesite detener e iniciar el servicio en determinadas situaciones.
- Desinstalación de servicio de gestión de clientes
Si ya no tiene que recopilar información de diagnóstico de cliente, puede desinstalar el servicio de gestión de clientes del sistema cliente.
- Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas
El servicio de gestión de clientes utiliza información del archivo de configuración de cliente (client-configuration.xml) para descubrir información de diagnóstico. Si el servicio de gestión de clientes no puede descubrir la ubicación de los archivos de registro, debe ejecutar el programa de utilidad CmsConfig para añadir la ubicación de los archivos de registro al archivo client-configuration.xml.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalación de servicio de gestión de clientes utilizando el asistente gráfico

Para recopilar información de diagnóstico sobre los clientes de archivado y copia de seguridad, por ejemplo archivos de registro de cliente, debe instalar el servicio de gestión de clientes en los sistemas cliente que gestiona.

Antes de empezar

Revise Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect.

Acerca de esta tarea

Debe instalar el servicio de gestión de clientes en el mismo sistema que el cliente de archivado y copia de seguridad.

Procedimiento

1. Descargue el paquete de instalación para el servicio de gestión de clientes de un sitio de descarga de IBM®, por ejemplo IBM Passport Advantage o IBM Fix Central. Busque un nombre de archivo que sea similar a `<version>-IBM-SPCMS-<sistema operativo>.bin`.

La tabla siguiente muestra los nombres de los paquetes de instalación.

Sistema operativo del cliente	Nombre de paquete de instalación
Linux x86 de 64 bits	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows de 32 bits	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows de 64 bits	8.1.x.000-IBM-SPCMS-Windows64.exe

2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
3. Extraiga el contenido del archivo del paquete de instalación.
 - En sistemas cliente Linux, lleve a cabo los siguientes pasos:
 - a. Ejecute el siguiente mandato para cambiar un archivo en un archivo ejecutable:


```
chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
```
 - b. Emita el mandato siguiente:


```
./8.1.x.000-IBM-SPCMS-Linuxx64.bin
```
 - En sistemas cliente de Windows, haga doble clic en el nombre del paquete de instalación en Windows Explorer.
Consejo: Si anteriormente ha instalado y desinstalado el paquete, seleccione All cuando se le solicite que sustituya los archivos de instalación existentes.
4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
 - En los sistemas cliente Linux, emita el mandato siguiente:

```
./install.sh
```




- o En sistemas cliente Windows, efectúe una doble pulsación en install.bat.
5. Para instalar el servicio de gestión de clientes, siga las instrucciones del asistente de IBM Installation Manager.

Si IBM Installation Manager aún no está instalado en el sistema cliente, tiene que seleccionar IBM Installation Manager e IBM Spectrum Protect Client Management Services.

Consejo: Puede aceptar las ubicaciones predeterminadas para el directorio de recursos compartidos y el directorio de instalación para IBM Installation Manager.

Qué hacer a continuación

Siga las instrucciones de Verificación de que el servicio de gestión de clientes está instalado correctamente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Instalación de servicio de gestión de clientes en modalidad silenciosa

Puede instalar el servicio de gestión de clientes en modalidad silenciosa. Cuando se utiliza la modalidad silenciosa, se proporcionan los valores de instalación en un archivo de respuestas y, a continuación, se ejecuta un mandato de instalación.

Antes de empezar

Revise Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect.

Extraiga el paquete de instalación siguiendo las instrucciones de Instalación de servicio de gestión de clientes utilizando el asistente gráfico.

Acerca de esta tarea

Debe instalar el servicio de gestión de clientes en el mismo sistema que el cliente de archivado y copia de seguridad.

El directorio input, que está en el directorio donde se ha extraído el paquete de instalación, contiene el siguiente archivo de respuestas de ejemplo:

```
install_response_sample.xml
```

Puede utilizar el archivo de ejemplo con los valores predeterminados o puede personalizarlo.

Consejo: Si desea personalizar el archivo de ejemplo, cree una copia del archivo de ejemplo, cámbiele el nombre y edite la copia.

Procedimiento

1. Cree un archivo de respuestas basado en el archivo de ejemplo o utilice el archivo de ejemplo, install_response_sample.xml. En cualquiera de los casos, asegúrese de que el archivo de respuestas especifica el número de puerto para el servicio de gestión de clientes. El puerto predeterminado es 9028. Por ejemplo:

```
<variable name='port' value='9028' />
```

2. Ejecute el mandato para instalar el servicio de gestión de clientes y acepte la licencia. Desde el directorio en donde se extrae el archivo del paquete de instalación, emita el siguiente mandato, donde *archivo_respuestas* representa la vía de acceso del archivo de respuesta, incluyendo el nombre de archivo:

En un sistema cliente Linux:

```
./install.sh -s -input response_file -acceptLicense
```

Por ejemplo:

```
./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
```

En un sistema cliente Windows:




```
install.bat -s -input response_file -acceptLicense
```

Por ejemplo:

```
install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
```

Qué hacer a continuación

Siga las instrucciones de Verificación de que el servicio de gestión de clientes está instalado correctamente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de clientes para recopilar información de diagnóstico acerca de un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de clientes esté instalado y configurado correctamente.

Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

```
dir_instalación_cliente/cms/bin/CmsConfig.sh list
```

donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME  
Capabilities: [LOG_QUERY]  
  Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys  
  
  Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log  
            en_US MM/dd/aaaa HH:mm:ss Windows-1252  
  
  Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log  
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

- En los sistemas cliente Windows, emita el mandato siguiente:

```
dir_instalación_cliente\cms\bin\CmsConfig.bat list
```

donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
C:\"Archivos de programa"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME  
Capabilities: [LOG_QUERY]  
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt  
  
  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log  
            en_US MM/dd/aaaa HH:mm:ss Windows-1252  
  
  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log  
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:




- En sistemas cliente de Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo client-configuration.xml. Para obtener instrucciones sobre cómo configurar este archivo, consulte Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato CmsConfig verify para verificar que se ha creado correctamente una definición de nodo en el archivo client-configuration.xml.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes

Si no ha utilizado la configuración predeterminada para el servicio de gestión de clientes, debe configurar el Centro de operaciones para acceder al servicio de gestión de clientes.

Antes de empezar

Asegúrese de que el servicio de gestión de clientes se ha instalado e iniciado en el sistema cliente.

Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de clientes no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
 - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse en una red, mientras que el servicio de gestión de clientes se comunica en la otra red.
 - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, al sistema cliente se le asigna dinámicamente una dirección IP, que se guarda en el servidor de IBM Spectrum Protect durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

Procedimiento

Para configurar el Centro de operaciones para utilizar el servicio de gestión de clientes, realice los pasos siguientes:

1. En la página Clientes del Centro de operaciones, seleccione el cliente.
2. Pulse Detalles.
3. Pulse el separador Propiedades.
4. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de clientes en el sistema cliente.



La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	<code>https://server.example.com</code>
Con el nombre de host de DNS y puerto no predeterminado	<code>https://server.example.com:1599</code>
Con la dirección IP y puerto no predeterminado	<code>https://192.0.2.0:1599</code>

5. Pulse Guardar.

Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Inicio y detención del servicio de gestión de clientes

El servicio de gestión de clientes se inicia automáticamente después de instalarse en el sistema cliente. Es posible que necesite detener e iniciar el servicio en determinadas situaciones.




Procedimiento

- Para detener, iniciar o reiniciar el servicio de gestión de clientes en sistemas cliente Linux, emita los mandatos siguientes:
 - Para detener el servicio:

```
service cms.rc stop
```
 - Para iniciar el servicio:

```
service cms.rc start
```
 - Para reiniciar el servicio:

```
service cms.rc restart
```
- En sistemas cliente Windows, abra la ventana Servicios y detenga, inicie o reinicie el servicio IBM Spectrum Protect Client Management Services.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Desinstalación de servicio de gestión de clientes

Si ya no tiene que recopilar información de diagnóstico de cliente, puede desinstalar el servicio de gestión de clientes del sistema cliente.

Acerca de esta tarea



Debe utilizar IBM® Installation Manager para desinstalar el servicio de gestión de clientes. Si ya no piensa utilizar IBM Installation Manager, también puede desinstalarlo.

Procedimiento

1. Desinstale el servicio de gestión de clientes del sistema cliente:
 - a. Abra IBM Installation Manager:
 - En el sistema cliente Linux, en el directorio donde está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente:

```
./IBMIM
```
 - En el sistema cliente Windows, abra IBM Installation Manager desde el menú Inicio.
 - b. Pulse en Desinstalar.
 - c. Seleccione IBM Spectrum Protect Client Management Services y pulse Siguiente.
 - d. Pulse Desinstalar y, a continuación, pulse Finalizar.
 - e. Cierre la ventana de IBM Installation Manager.
2. Si ya no necesita IBM Installation Manager, desinstálelo del sistema cliente:
 - a. Abra el asistente de desinstalación de IBM Installation Manager:
 - En el sistema cliente Linux, cambie al directorio de desinstalación de IBM Installation Manager (por ejemplo /var/ibm/InstallationManager/uninstall) y emita el mandato siguiente:

```
./uninstall
```
 - En el sistema cliente Windows, pulse Inicio > Panel de control. A continuación, pulse Desinstalar un programa > IBM Installation Manager > Desinstalar.
 - b. En la ventana de IBM Installation Manager, seleccione IBM Installation Manager si aún no está seleccionado y pulse Siguiente.
 - c. Pulse Desinstalar y pulse Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas



El servicio de gestión de clientes utiliza información del archivo de configuración de cliente (client-configuration.xml) para descubrir información de diagnóstico. Si el servicio de gestión de clientes no puede descubrir la ubicación de los archivos de registro, debe ejecutar el programa de utilidad CmsConfig para añadir la ubicación de los archivos de registro al archivo client-configuration.xml.


- Programa de utilidad CmsConfig
Si no está utilizando la configuración de cliente predeterminada, puede ejecutar el programa de utilidad CmsConfig en el sistema cliente para descubrir y añadir la ubicación de los archivos de registro de cliente al archivo client-configuration.xml. Después de completar la configuración, el servicio de gestión de clientes puede acceder a los archivos de registro de cliente y dejarlos disponibles para las funciones básicas de diagnóstico en el Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux

Resolución de problemas de la instalación de Centro de operaciones

Si ocurre un problema con la instalación del Centro de operaciones y no puede resolverlo, puede consultar las descripciones de problemas conocidos para una posible solución.

-  Sistemas operativos AIX El asistente de instalación gráfica no puede iniciarse en un sistema AIX
Está instalando Centro de operaciones en un sistema AIX haciendo uso del asistente gráfico, y el programa de instalación no se inicia.
-  Sistemas operativos Linux Las letras en chino, japonés o coreano se muestran incorrectamente
Las fuentes en chino, japonés o coreano se muestran incorrectamente en Centro de operaciones en Red Hat Enterprise Linux 5.

 Sistemas operativos AIX

El asistente de instalación gráfica no puede iniciarse en un sistema AIX

Está instalando Centro de operaciones en un sistema AIX haciendo uso del asistente gráfico, y el programa de instalación no se inicia.

Solución

Los archivos RPM que aparecen en Instalación de Centro de operaciones utilizando el asistente gráfico deben estar instalados en el sistema. Compruebe que los archivos RPM estén instalados.

 Sistemas operativos Linux

Las letras en chino, japonés o coreano se muestran incorrectamente

Las fuentes en chino, japonés o coreano se muestran incorrectamente en Centro de operaciones en Red Hat Enterprise Linux 5.

Solución

Instale los siguientes paquetes de fuentes, que están disponibles en Red Hat:

- fonts-chinese
- fonts-japanese
- fonts-korean

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Desinstalación de Centro de operaciones

Puede desinstalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.



- Desinstalación de Centro de operaciones utilizando el asistente gráfico
Puede desinstalar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.
- Desinstalación del Centro de operaciones en modalidad de consola
Para desinstalar Centro de operaciones mediante el uso de la línea de mandatos, debe ejecutar el programa de desinstalación IBM Installation Manager desde la línea de mandato con el parámetro para la modalidad de consola.
- Desinstalar Centro de operaciones en modalidad silenciosa
Para desinstalar Centro de operaciones en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros de la modalidad silenciosa.

Desinstalación de Centro de operaciones utilizando el asistente gráfico


Puede desinstalar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.

Procedimiento




1. Abra IBM Installation Manager.

 Sistemas operativos AIX  Sistemas operativos Linux En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:

```
./IBMIM
```

 Sistemas operativos Windows Puede abrir IBM Installation Manager desde el menú Inicio.




2. Pulse en Desinstalar.
3. Seleccione la opción para Centro de operaciones y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




Desinstalación del Centro de operaciones en modalidad de consola




Para desinstalar Centro de operaciones mediante el uso de la línea de mandatos, debe ejecutar el programa de desinstalación IBM® Installation Manager desde la línea de mandato con el parámetro para la modalidad de consola.

Procedimiento

1. En el directorio en el que está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
 - o  Sistemas operativos AIX  Sistemas operativos Linux eclipse/tools
 - o  Sistemas operativos Windows eclipse\tools

Por ejemplo:

- o  Sistemas operativos AIX  Sistemas operativos Linux /opt/IBM/InstallationManager/eclipse/tools
- o  Sistemas operativos Windows C:\Archivos de programa\IBM\Installation Manager\eclipse\tools

2. Desde el directorio herramientas, emita el siguiente mandato:
 - o  Sistemas operativos AIX  Sistemas operativos Linux ./imcl -c
 - o  Sistemas operativos Windows imcl.exe -c
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique **N** para Siguiente.
6. Elija desinstalar el paquete de Centro de operaciones.
7. Especifique **N** para Siguiente.
8. Escriba **U** para Desinstalar.
9. Escriba **F** para Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Desinstalar Centro de operaciones en modalidad silenciosa

Para desinstalar Centro de operaciones en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros de la modalidad silenciosa.

Antes de empezar




Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa el servidor de Centro de operaciones. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Para desinstalar el Centro de operaciones, deje establecido `modify="false"` para la entrada del Centro de operaciones en el archivo de respuestas.




Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

Procedimiento




1. En el directorio en el que está instalado IBM Installation Manager, vaya al siguiente subdirectorio:

-  Sistemas operativos AIX  Sistemas operativos Linux/eclipse/tools
-  Sistemas operativos Windows/eclipse/tools




Por ejemplo:


-  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
-  Sistemas operativos Windows C:\Archivos de programa\IBM\Installation Manager\eclipse/tools

2. Desde el directorio herramientas, emita el siguiente mandato, donde *response_file* representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

-  Sistemas operativos AIX  Sistemas operativos Linux./imcl -input *archivo_respuestas* -silent
-  Sistemas operativos Windows imcl.exe -input *archivo_respuestas* -silent

El siguiente mandato es un ejemplo:

-  Sistemas operativos AIX  Sistemas operativos Linux./imcl -input /tmp/input/uninstall_response.xml -silent
-  Sistemas operativos Windows imcl.exe -input C:\tmp\input\uninstall_response.xml -silent

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Volver a una versión anterior de Centro de operaciones

De forma predeterminada, IBM® Installation Manager guarda versiones anteriores de un paquete para poder regresar a una versión anterior si experimenta un problema con versiones posteriores de actualizaciones, arreglos o paquetes.

Antes de empezar

La función de restauración está disponible solo cuando Centro de operaciones está actualizado.

Acerca de esta tarea

Cuando IBM Installation Manager restaura un paquete a una versión anterior, la versión actual de los archivos del paquete se desinstala, y se vuelve a instalar una versión anterior.

Para restaurar a una versión anterior, IBM Installation Manager debe acceder a los archivos de esa versión. De manera predeterminada, estos archivos se guardan durante cada instalación sucesiva. Debido al número de archivos guardados con cada versión instalada, es posible que quiera eliminar estos archivos del sistema de forma regular. Sin embargo, si elimina los archivos, no puede regresar a la versión anterior.

Para eliminar archivos guardados o para actualizar su preferencia para guardar estos archivos en instalaciones futuras, siga estos pasos:

1. En IBM Installation Manager, pulse Archivo > Preferencias.
2. En la página de Preferencias, pulse Archivos a restaurar y especifique su preferencia.

Procedimiento

Para restaurar una versión anterior de Centro de operaciones, use la función Retrotraer de IBM Installation Manager.

Configuración de servidores

Para completar las tareas de configuración para el servidor de IBM Spectrum Protect, revise la documentación disponible.

Acerca de esta tarea

Para una solución existente, revise las acciones siguientes.

Para planificar, implementar, supervisar y utilizar una nueva solución, siga las instrucciones de Soluciones de protección de datos de IBM Spectrum Protect.

Consejo: A partir de IBM Spectrum Protect V7.1.3, la *Guía del administrador* ha quedado obsoleta.

Acción	Detalles	Documentación
Supervisión de una solución de almacenamiento	Supervise la solución de almacenamiento para identificar problemas potenciales y existentes. De este modo, puede resolver problemas y optimizar el rendimiento del sistema.	Supervisión de soluciones de almacenamiento
Selección y configuración de almacenamiento	Seleccione el almacenamiento en función de las necesidades de la empresa y realice las tareas de configuración.	Configuración del almacenamiento
Eliminar datos duplicados	<p>Utilice la eliminación de datos duplicados para eliminar datos redundantes en las agrupaciones de almacenamiento. La eliminación de duplicados de datos reduce el almacenamiento necesario para conservar los datos. En una agrupación de almacenamiento cuyos duplicados se han eliminado sólo se conserva una instancia de los datos.</p> <p>Con IBM Spectrum Protect versión 7.1.3 y posteriores, puede utilizar la eliminación de duplicados de datos en línea.</p>	Para obtener más información sobre las diferencias entre la eliminación de duplicados de datos en línea y postproceso, y para configurar la solución de mejores prácticas para la eliminación de duplicados de datos, consulte Opciones de eliminación de datos duplicados.
Replicar datos	Puede replicar datos de nodo de cliente desde un servidor de réplica fuente a un servidor de réplica de destino. Si se produce un desastre y el servidor de origen no está disponible temporalmente, los nodos de cliente pueden recuperar los datos del servidor de réplica de destino.	<p>Para implementar una solución de mejores prácticas que utilice la duplicación y la migración tras error automática IBM Spectrum Protect, consulte el apartado Solución de disco multisitio.</p> <p>Para obtener información general acerca de la réplica, incluidos los pasos de configuración, consulte Réplica de datos de cliente en otro servidor.</p>
Gestionar la base de datos y las anotaciones de recuperación	La base de datos y el registro de recuperación o el inventario del servidor, almacenan información sobre datos de cliente y son esenciales para el funcionamiento del servidor.	<ul style="list-style-type: none"> • Para obtener información general acerca de la base de datos y registro de recuperación, consulte: Gestión de la base de datos y el registro de recuperación (V7.1.1). • Para optimizar la reorganización de índices y tablas de la base de datos del servidor, y evitar y resolver problemas relacionados con el aumento de la base de datos y el rendimiento, consulte nota técnica 1683633.
Proteger el servidor	Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.	Protección del servidor IBM Spectrum Protect

Acción	Detalles	Documentación
Configure SSL para LDAP (Lightweight Directory Access Protocol)	Puede configurar SSL para los servidores de directorios LDAP y gestionar las contraseñas y los procedimientos de inicio de sesión.	Para obtener información sobre LDAP, consulte: <ul style="list-style-type: none"> • Autenticación de los usuarios mediante un servidor LDAP • Configuración de SSL o TLS para los servidores de directorio LDAP (V7.1.1)
Obtenga información y configure políticas para la retención de datos	Las políticas de IBM Spectrum Protect definen las reglas para gestionar los datos.	Para actualizar las políticas, utilice el Centro de operaciones. Para obtener más información sobre las políticas y crear políticas, consulte Personalización de políticas.
Protección del servidor y recuperación después de un desastre	Proteja la infraestructura del sistema y de los datos para que pueda recuperarlos después de un desastre. Utilice las herramientas y procedimientos que proporciona IBM Spectrum Protect para ayudarlo a crear un plan de recuperación tras desastre.	Para obtener información sobre cómo proteger y recuperar el servidor, consulte: <ul style="list-style-type: none"> • Protección de los archivos de configuración de infraestructura y base de datos (V7.1.1) • Utilización del gestor de recuperación ante siniestro para entornos de cinta (V7.1.1)
Proteger servidores de archivos NAS	Puede planificar, configurar y gestionar un entorno de copia de seguridad que proteja su servidor de archivos de almacenamiento adjunto de red (NAS).	Protección de servidores de archivos NAS
Configurar un entorno en clúster	Configure un entorno en clúster en AIX, Linux, o Windows para garantizar una mayor disponibilidad del servidor y minimizar el tiempo de inactividad.	Configuración de entornos en clúster
Verificación de conformidad de la licencia	Verifique que la solución de IBM Spectrum Protect cumple las condiciones del acuerdo de licencia. Si comprueba el cumplimiento de forma periódica, podrá realizar un seguimiento de las tendencias del crecimiento de los datos o el uso del value unit de procesador (PVU).	Verificación de la conformidad de licencia

- Protección del servidor IBM Spectrum Protect
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- Réplica de datos de cliente en otro servidor
El hecho de realizar una réplica de los datos de cliente de un servidor de origen en otro servidor ayuda a garantizar que los datos de cliente copiados están disponibles para su recuperación si el servidor de origen resulta dañado. La réplica realiza una copia incremental de los datos del servidor de origen en el servidor de destino para proporcionar capacidad de migración y recuperación.
- Configuración de entornos en clúster
Puede configurar el servidor de IBM Spectrum Protect para la agrupación en clúster en sistemas AIX, Linux o Windows.

Protección del servidor IBM Spectrum Protect

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- **Conceptos sobre la seguridad**
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- **Gestión de administradores**
Un administrador con autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas de las tareas debe tener asignados uno o varios niveles de autorización.
- **Cambio de los requisitos de contraseña**
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- **Protección de IBM Spectrum Protect en el sistema**
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.
- **Protección del entorno de almacenamiento contra el ransomware**
Los entornos de almacenamiento conectados a internet pueden ser el objetivo de ataques de ransomware. Puede llevar a cabo pasos para proteger su entorno de almacenamiento contra el ransomware y asegurarse de que podrá recuperar sus servidores y clientes si se produce un ataque.
- **Protección de las comunicaciones**
Sus datos y contraseñas son más seguros si los protege mediante Secure Sockets Layer (SSL) o Transport Layer Security (TLS), una forma de SSL.
- **Autenticación de los usuarios de IBM Spectrum Protect mediante un servidor LDAP**
En un sistema IBM Spectrum Protect, los usuarios deben autenticarse en el servidor proporcionando un ID de usuario y contraseña. Si su organización utiliza un servidor LDAP (Lightweight Directory Access Protocol) para gestionar los ID de usuario, puede utilizar el servidor LDAP para autenticar los ID de usuario de IBM Spectrum Protect.

Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

Seguridad de la capa de transporte

Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 utilizada por cualquier servidor de IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

Niveles de autorización

En cada servidor de IBM Spectrum Protect, hay diferentes niveles de autorización administrativa disponibles que determinan las tareas que puede llevar a cabo un administrador.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos o eliminarlos, y bloquearlos y desbloquearlos del servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. De forma predeterminada, un ID de usuario no root no puede hacer copia de seguridad de los datos en el nodo. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben entrar una contraseña cuando acceden al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Autenticación de los usuarios mediante un servidor LDAP.

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días. El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña dentro de este período, se deberá cambiar la contraseña la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente, los clientes administrativos y los servidores de IBM Spectrum Protect y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT, y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos cliente	<ul style="list-style-type: none"> • REGISTER NODE • UPDATE NODE
Administradores	<ul style="list-style-type: none"> • REGISTER ADMIN • UPDATE ADMIN
Servidores	<ul style="list-style-type: none"> • DEFINE SERVER • UPDATE SERVER

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar utilizando una versión anterior, una vez que se han autenticado utilizando V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:
Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el

certificado esté instalado en todos ellos.

- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel más elevado de seguridad para la comunicación con el servidor de IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores utilicen la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

Referencia relacionada:

Protección de las comunicaciones

SELECT (Realizar una consulta SQL de la base de datos)

Gestión de administradores

Un administrador con autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas de las tareas debe tener asignados uno o varios niveles de autorización.

Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente: a. Registre el administrador y especifique Pa\$#\$twO como contraseña ejecutando el siguiente mandato: <pre>register admin admin1 Pa\$#\$twO</pre> b. Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre>
Cambie los permisos del administrador.	Cambie el nivel de autorización de un administrador, ADMIN1. • Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> • Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <pre>revoke authority admin1 classes=system</pre>
Elimine administradores.	Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect: <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.

Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</p> <p>c. Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</p> <p>El valor predeterminado en la instalación es 0.</p>
Establecer una longitud mínima para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establezca el número de caracteres en el campo Longitud mínima de contraseña.</p>
Establecer el período de caducidad para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establecer el número de días en el campo Caducidad común de la contraseña.</p>
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben escribir una contraseña para acceder al servidor.</p> <p>Sólo se puede inhabilitar la autenticación por contraseña para las contraseñas que se autentican con el servidor (LOCAL). Si se inhabilita la autenticación de contraseña, puede aumentar el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como método de autenticación predeterminado, emita el mandato siguiente:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para que se autentique con el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

Protección de IBM Spectrum Protect en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios de la base de datos del servidor ni a la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un

administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

- Limitación de acceso a través de restricciones de puerto
Limite el acceso al servidor aplicando restricciones de puerto.

Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
 - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
 - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grave en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique el parámetro BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Limitación de acceso a través de restricciones de puerto

Limite el acceso al servidor aplicando restricciones de puerto.

Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPPORT. Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPORT y SSLTCPPOINT.
SSLTCPPOINT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.

Opción de servidor	Acceso de puerto
SSLTCPADMINPORT	<p>Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.</p> <p>Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPOINT y SSLTCPPOINT.</p>

Restricciones:

Las siguientes restricciones se aplican cuando se especifican los puertos de servidor sólo para SSL (SSLTCPPOINT y SSLTCPADMINPORT):

- Cuando especifique el puerto sólo para SSL del servidor para LLADDRESS en el mandato DEFINE SERVER o UPDATE SERVER, también debe especificar el parámetro SSL=YES.
- Cuando especifique el puerto sólo para SSL del servidor para la opción TCPPOINT del cliente, también debe especificar YES para la opción del cliente SSL.

Protección del entorno de almacenamiento contra el ransomware

Los entornos de almacenamiento conectados a internet pueden ser el objetivo de ataques de ransomware. Puede llevar a cabo pasos para proteger su entorno de almacenamiento contra el ransomware y asegurarse de que podrá recuperar sus servidores y clientes si se produce un ataque.

Acerca de esta tarea

El *ransomware* es un software malicioso que se utiliza para obtener acceso a un sistema informático y cifrar los datos. Normalmente el iniciador de un ataque de ransomware cifra los datos y, a continuación, se pone en contacto con el propietario de los datos para pedir un rescate. Si no se paga dicho rescate, el iniciador del ataque amenaza con dejar los datos cifrados. Por esta razón, puede ayudar a proteger el entorno de almacenamiento contra un ataque de ransomware almacenando una copia de los datos en una ubicación que *no* sea accesible desde Internet.

Una posibilidad es realizar una copia de seguridad de la base de datos para grabar y respaldar a los clientes para copiar agrupaciones de almacenamiento en cintas y, a continuación, transportar los volúmenes de cinta a una ubicación segura y fuera de línea. Si utiliza esta estrategia, puede habilitar la función IBM Spectrum Protect gestor recuperación ante siniestro (DRM) para realizar el seguimiento de los medios fuera de línea y registrar dicha información en la base de datos de IBM Spectrum Protect. El DRM consolida planes, scripts y otra información en un archivo de plan. Puede utilizar el archivo de plan para recuperar sus servidores y clientes después de un ataque de ransomware.

Procedimiento

1. Cuando planea su entorno de almacenamiento, considere si utilizar la cinta como medio de almacenamiento y si transportar los volúmenes de cinta fuera del sitio. Para obtener instrucciones sobre cómo configurar el almacenamiento en cinta, consulte Solución de cinta.
2. Cuando planea su entorno de almacenamiento, considere si utilizar la función DRM para recuperarse de un ataque de ransomware, una parada no planificada o un desastre. Para obtener una introducción a DRM, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.
3. Revise las políticas definidas para su entorno de almacenamiento para asegurarse de que se retiene un número suficiente de copias de seguridad y que las copias se retienen durante suficientes días. Si el ransomware cifra sus archivos más recientes, todavía puede acceder a sus versiones anteriores. Para definir políticas, utilice Centro de operaciones o los mandatos DEFINE COPYGROUP y UPDATE COPYGROUP. Para obtener información sobre los valores preferidos, consulte Retención y caducidad de las versiones de copia de seguridad.
4. Supervise diariamente su sistema para detectar el ransomware tan pronto como sea posible. Para más información, consulte Lista de comprobación de supervisión diaria y Lista de comprobación de supervisión periódica.

Protección de las comunicaciones

Sus datos y contraseñas son más seguros si los protege mediante Secure Sockets Layer (SSL) o Transport Layer Security (TLS), una forma de SSL.

SSL y TLS son la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL y TLS proporcionan un canal seguro para que los clientes se comuniquen a través de vías de acceso de comunicación abiertas. Con SSL y TLS, la identidad del servidor se verifica mediante el uso de certificados digitales. Los clientes y servidores que utilicen IBM Spectrum Protect V8.1.2 o software de versiones posteriores para comunicarse se configurarán automáticamente para utilizar TLS 1.2. Los agentes de almacenamiento que

utilicen IBM Spectrum Protect V8.1.3 y software de versiones posteriores o Tivoli Storage Manager V7.1.8 o software de versiones posteriores también se configurarán automáticamente.

Nota: En V8.1.2, se deben configurar manualmente los agentes de almacenamiento para utilizar SSL.

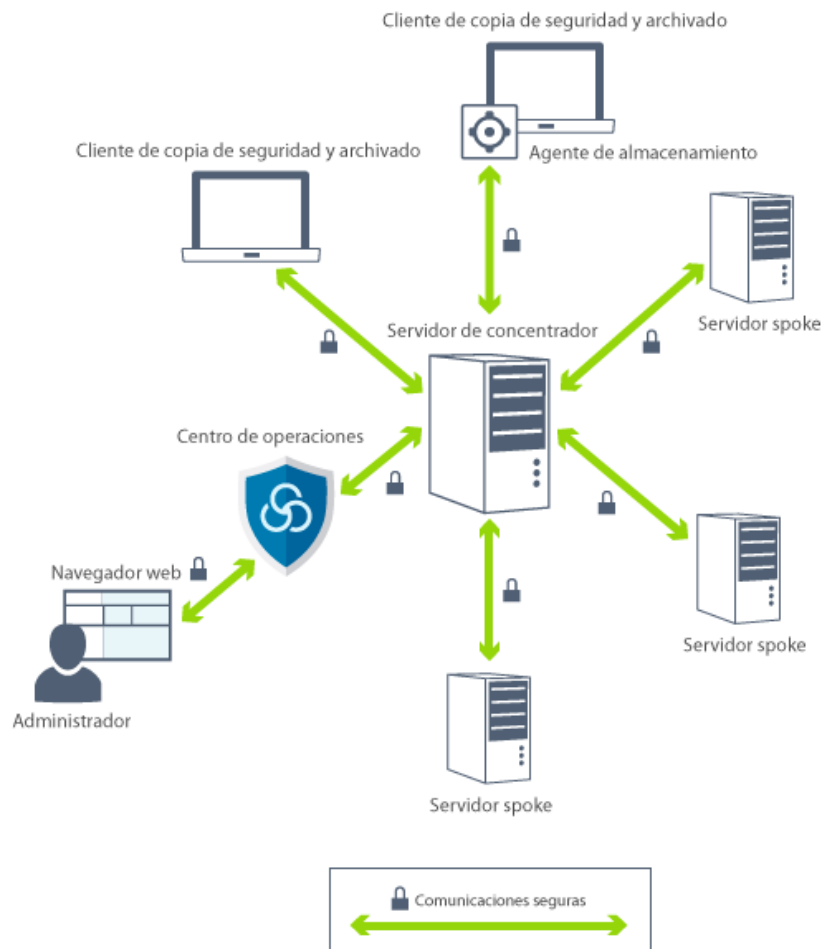
Para mejorar el rendimiento del sistema, utilice TLS para la autenticación sin cifrar datos de objetos. Para especificar si el servidor utiliza TLS 1.2 para toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor, y el parámetro SSL en el mandato UPDATE SERVER para la comunicación de servidor a servidor. Si elige utilizar TLS para cifrar datos de objetos, plantéese la posibilidad de añadir recursos de procesador adicionales en el servidor de IBM Spectrum Protect para gestionar el aumento del tráfico de red.

Si autentica las contraseñas con un servidor de directorios LDAP, TLS protege las contraseñas entre el servidor de IBM Spectrum Protect y el servidor LDAP. TLS es necesario para todas las comunicaciones de contraseñas LDAP.

- Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte
Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores de IBM Spectrum Protect, clientes, agentes de almacenamiento y el Centro de operaciones. Si envía datos entre el servidor el cliente y el agente de almacenamiento, se utiliza SSL o TLS para cifrar los datos.
- Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL
Configure la Capa de sockets seguros (SSL) en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad, el agente de almacenamiento y el Centro de operaciones para asegurarse de que los datos están cifrados durante la comunicación.

Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte

Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores de IBM Spectrum Protect, clientes, agentes de almacenamiento y el Centro de operaciones. Si envía datos entre el servidor el cliente y el agente de almacenamiento, se utiliza SSL o TLS para cifrar los datos.



Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con unas instancias de base de datos de IBM DB2 utilizada por el servidor IBM Spectrum Protect.

Cada servidor o agente de almacenamiento tiene una clave privada exclusiva y un certificado firmado exclusivo que se utiliza para permitir conexiones SSL. Si utiliza certificados autofirmados, debe distribuir el certificado autofirmado para cada servidor o agente de almacenamiento para todos los clientes, agentes de almacenamiento y servidores que utilizan TLS para comunicarse con él. Si utiliza certificados firmados por una entidad emisora de certificados, debe distribuir sólo los certificados de entidad emisora de certificados a todos los clientes, agentes de almacenamiento y servidores que utilizan TLS para comunicarse.

Si utiliza un certificado raíz de una entidad emisora de certificados, deberá instalarlo en cada base de datos de claves del cliente, servidor y agente de almacenamiento que inicie la comunicación SSL. Un *certificado raíz* es un certificado que identifica la entidad emisora de certificados raíz. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL.

El servidor IBM Spectrum Protect permite certificados CA firmados que sean SHA-256 o inferiores. Se recomiendan los certificados SHA-256 para mejorar la seguridad y cumplir con los estándares NIST. Se recomienda SHA-256 para comunicarse con el Centro de operaciones.

A partir de IBM Spectrum Protect Versión 8.1.2, SSL está habilitado de forma predeterminada para las comunicaciones entre servidores y clientes de V8.1.2. Los agentes de almacenamiento se configuran automáticamente para utilizar SSL a partir del software IBM Spectrum Protect V8.1.3 o posterior y del software Tivoli Storage Manager V7.1.8 o posterior.

Nota: En V8.1.2, se deben configurar manualmente los agentes de almacenamiento para utilizar SSL.

El servidor, cliente o agente de almacenamiento de IBM Spectrum Protect pueden servir como clientes SSL durante la comunicación. Un cliente SSL es el componente que inicia la comunicación y verifica el certificado para un servidor SSL. Por ejemplo, si el cliente de IBM Spectrum Protect inicia la comunicación SSL con el servidor de IBM Spectrum Protect, el cliente de IBM Spectrum Protect es el cliente SSL y el servidor es el servidor SSL.

Tabla 1 enumera los componentes, que pueden ser un cliente SSL o un servidor SSL.

Tabla 1. Servidores y clientes SSL del entorno de IBM Spectrum Protect

Cliente SSL	Servidor SSL	Escenario
-------------	--------------	-----------

Cliente SSL	Servidor SSL	Escenario
Cliente	Servidor	El cliente de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. El cliente verifica el certificado. El servidor proporciona el certificado.
Servidor (por ejemplo, un servidor de origen)	Servidor (por ejemplo, un servidor de destino)	El servidor de origen de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor de destino de IBM Spectrum Protect. El servidor de origen actúa como un cliente SSL y verifica el certificado que proporciona el servidor de destino. Este tipo de comunicación es común durante el proceso de réplica.
Cliente a través de un agente de almacenamiento	Servidor	El cliente comprueba cada certificado cuando inicia la comunicación SSL por separado con el servidor de IBM Spectrum Protect y el agente de almacenamiento. Cuando el agente de almacenamiento se comunica con el servidor utilizando el protocolo de comunicación SSL, el agente de almacenamiento actúa como un cliente SSL y verifica el certificado que proporciona el servidor. El agente de almacenamiento puede ser el cliente SSL y el proveedor de SSL al mismo tiempo.
Servidor	Servidor LDAP	El servidor de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor LDAP. El servidor de IBM Spectrum Protect actúa como un cliente SSL y verifica el certificado que proporciona el servidor LDAP.
Centro de operaciones	Servidor	El Centro de operaciones inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. El Centro de operaciones actúa como un cliente SSL y verifica el certificado que proporciona el servidor de IBM Spectrum Protect.
Informes	Servidor	El agente de creación de informes inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. La función de creación de informes actúa como un cliente SSL y verifica el certificado que proporciona el servidor de IBM Spectrum Protect.

Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL

Configure la Capa de sockets seguros (SSL) en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad, el agente de almacenamiento y el Centro de operaciones para asegurarse de que los datos están cifrados durante la comunicación.

Puede utilizar un certificado SSL autofirmado o un certificado firmado por una entidad emisora de certificados (CA) de terceros para verificar una solicitud de comunicación SSL entre el servidor, el cliente y el agente de almacenamiento. Cada servidor, cliente o agente de almacenamiento de IBM Spectrum Protect que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo firmado por una entidad emisora de certificados.

La ventaja de los certificados firmados por una entidad emisora de certificados es que un único certificado firmado por entidad emisora de certificados se puede utilizar para todos los servidores, lo que le permite distribuir un solo certificado a los clientes. Si utiliza un certificado autofirmado, el certificado se crea automáticamente para cada servidor y agente de almacenamiento. Si utiliza un certificado raíz de una entidad emisora de certificados, deberá instalarse en cada base de datos de claves del cliente, servidor y agente de almacenamiento que inicie la comunicación SSL. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL.

Restricción: Algunas entidades emisoras de certificados utilizan certificados en un formato que no reconoce IBM Spectrum Protect. Es posible que necesite contactar con la entidad emisora de certificados para convertir el certificado a un formato que pueda utilizar con IBM Spectrum Protect.

- Configuración del servidor para aceptar conexiones SSL
Configure el servidor para que acepte conexiones SSL antes de habilitar la comunicación SSL desde el servidor a un cliente, un agente de almacenamiento u otro servidor.
- Configuración de un agente de almacenamiento para utilizar SSL
Para asegurarse de que los datos se cifran durante la comunicación entre el agente de almacenamiento y el servidor y el agente de almacenamiento y el cliente, configure los agentes de almacenamiento para la comunicación utilizando el protocolo SSL.
- Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL
Para proteger los datos que se transmiten entre un cliente y un agente de almacenamiento, configure el cliente para conectarse al agente de almacenamiento mediante el protocolo SSL.

Configuración del servidor para aceptar conexiones SSL

Configure el servidor para que acepte conexiones SSL antes de habilitar la comunicación SSL desde el servidor a un cliente, un agente de almacenamiento u otro servidor.

Procedimiento

1. Especifique el puerto en el que el servidor espera comunicaciones de cliente habilitadas para SSL o acepte el número de puerto predeterminado. Opcionalmente, actualice el archivo `dsmserv.opt` en el directorio de instancia del servidor especificando la opción `TCPSPORT` o `TCPADMINPORT`, o ambas. Se pueden utilizar las opciones `SSLTCPSPORT` y `SSLTCPADMINPORT` para conexiones SSL solamente.
2. Cree una base de datos de claves de servidor iniciando el servidor. El archivo de base de datos de claves de servidor, `cert.kdb`, se almacena en el directorio de instancia de servidor, y la etiqueta de certificado predeterminada se define automáticamente como "TSM Server SelfSigned SHA Key". El certificado se exporta al archivo `cert256.arm`.
3. Si utiliza el certificado autofirmado predeterminado, se requerirá el archivo de certificado autofirmado predeterminado (`cert256.arm`) cuando se conecte al servidor utilizando TLS.
4. Si está importando un certificado firmado por una entidad emisora de certificados, realice los siguientes pasos:

- a. Importe un certificado exclusivo firmado por una entidad emisora de certificados en cada servidor que habilite SSL. Puede importar un certificado firmado por CA intermediario o raíz. El mismo certificado firmado por CA se utiliza para todos los servidores. Inicie sesión en el sistema del servidor de IBM Spectrum Protect con el ID de usuario de instancia y emita el siguiente mandato de ejemplo desde el directorio de instancia:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed -label "CA cert" -file ca.crt
```

- b. Para importar un certificado firmado por entidad emisora de certificados intermedio, emita el siguiente mandato de ejemplo:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed  
-label "Intermediate CA cert" -file intca.crt
```

- c. Se requerirán los certificados intermedio y raíz (`ca.crt` y `intca.crt`) cuando se conecte al servidor utilizando TLS.
- d. En el servidor, cree una solicitud de certificado para que lo firme la entidad emisora de certificados emitiendo un mandato similar al siguiente mandato:

```
gsk8capiCmd_64 -certreq -create -db cert.kdb -stashed -label "CA cert"  
-sigalg sha256 -size 2048 -ku "digitalSignature,keyEncipherment,keyAgreement "  
-eku "clientAuth,serverAuth" -dn "CN=tucson.example.com,OU=Spectrum Protect,O=IBM"  
-san_dnsname tucson.example.com -san_ipaddr 9.11.0.0 -file cert_request.csr
```

- e. Para recibir el certificado firmado y convertirlo en el certificado predeterminado para la comunicación con los clientes, emita el siguiente mandato de ejemplo:

```
gsk8capiCmd_64 -cert -receive -db cert.kdb -stashed -file cert_signed.crt  
-default_cert yes
```

5. Si realiza cambios, reinicie el servidor.

Qué hacer a continuación

Habilite la comunicación SSL desde un cliente, un agente de almacenamiento u otro servidor a este servidor. Para completar las siguientes tareas, debe tener un certificado del servidor y el número de puerto que se define para el servidor.

1. Para habilitar la comunicación SSL de un cliente a este servidor, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con la capa de sockets seguros.
2. Para habilitar la comunicación SSL desde otro servidor a este servidor, consulte Configuración del servidor para conectarse a otro servidor utilizando SSL.
3. Para habilitar la comunicación SSL desde un agente de almacenamiento a este servidor, consulte Configuración de un agente de almacenamiento para utilizar SSL.
4. Para habilitar la comunicación SSL desde el Centro de operaciones a este servidor, consulte Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL.

- Configuración de clientes para comunicarse con el servidor utilizando SSL
Para asegurarse de que los datos se cifra durante la comunicación entre clientes y servidor, configure los clientes para la comunicación con el servidor utilizando el protocolo SSL.
- Configuración del servidor para conectarse a otro servidor utilizando SSL
Para asegurarse de que los datos se cifran durante la comunicación de servidor a servidor, configure los servidores para la comunicación con servidores utilizando el protocolo SSL.
- Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL
Para asegurarse de que los datos se cifran durante la comunicación entre el Centro de operaciones y el servidor, configure el Centro de operaciones para la comunicación con el servidor utilizando el protocolo SSL.

Referencia relacionada:

TCPSPORT
TCPADMINPORT
QUERY SESSION (Consultar sesiones de cliente)

Configuración de clientes para comunicarse con el servidor utilizando SSL

Para asegurarse de que los datos se cifra durante la comunicación entre clientes y servidor, configure los clientes para la comunicación con el servidor utilizando el protocolo SSL.

Antes de empezar

Debe tener el certificado del servidor y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

Procedimiento

Para habilitar la comunicación SSL entre el servidor y los clientes, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con la capa de sockets seguros.

Configuración del servidor para conectarse a otro servidor utilizando SSL

Para asegurarse de que los datos se cifran durante la comunicación de servidor a servidor, configure los servidores para la comunicación con servidores utilizando el protocolo SSL.

Antes de empezar

Debe tener el certificado y el número de puerto para el servidor al que se va a conectar. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

Acerca de esta tarea

Sugerencias:

- Si ambos servidores utilizan el software IBM Spectrum Protect V8.1.2 o posterior, SSL se configura automáticamente. Se recomienda la configuración manual, aunque no es obligatoria. Si alguno de los servidores utiliza software IBM Spectrum Protect anterior a V8.1.2 o software Tivoli Storage Manager anterior a V7.1.8, deberá configurar manualmente SSL.
- En V8.1.2, se deben configurar manualmente los agentes de almacenamiento para utilizar SSL. En V8.1.3, los agentes de almacenamiento se configuran automáticamente para utilizar SSL.

En el procedimiento, se utilizan las siguientes direcciones de servidor como ejemplos:

- ServerA (el servidor al que se conecta) está en `bfa.tucson.example.com`
- ServerB está en `bfbb.tucson.example.com`

Procedimiento

1. Cree una base de datos de claves de servidor iniciando el servidor. El archivo de base de datos de claves del servidor, `cert.kdb`, se almacena en el directorio de instancia del servidor.
2. Para cada servidor, importe los archivos de certificado de entidad emisora de certificados o `cert256.arm` del otro servidor:

```
gsk8capicmd_64 -cert -add -label server_ip_address -db cert.kdb -stashed  
-file cert256.arm
```

Consejo: Utilice la dirección IP del servidor como el nombre de la etiqueta.

3. En cada servidor, puede ver los certificados de la base de datos de claves con el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

4. Reinicie los servidores.
5. Emita el mandato DEFINE SERVER.
 - a. Para ServerA, emita el siguiente mandato:

```
DEFINE SERVER BFB hla=bfbb.tucson.example.com lla=1542  
serverpa=passwordforbfb SSL=YES
```

b. Para ServerB, emita el siguiente mandato:

```
DEFINE SERVER BFA hla=bfa.tucson.example.com lla=1542
serverpa=passwordforbfa SSL=YES
```

Referencia relacionada:

QUERY SESSION (Consultar sesiones de cliente)

TCPPORT

TCPADMINPORT

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL

Para asegurarse de que los datos se cifran durante la comunicación entre el Centro de operaciones y el servidor, configure el Centro de operaciones para la comunicación con el servidor utilizando el protocolo SSL.

Antes de empezar

Debe tener el certificado del servidor concentrador y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

Procedimiento

Para configurar las comunicaciones SSL con el Centro de operaciones, consulte Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

Configuración de un agente de almacenamiento para utilizar SSL

Para asegurarse de que los datos se cifran durante la comunicación entre el agente de almacenamiento y el servidor y el agente de almacenamiento y el cliente, configure los agentes de almacenamiento para la comunicación utilizando el protocolo SSL.

Antes de empezar

Debe tener el certificado del servidor y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

Procedimiento

1. Inicialice el agente de almacenamiento y añada información de comunicación al archivo de configuración de dispositivo y al archivo de opciones del agente de almacenamiento `dsmsta.opt`, emitiendo el mandato `DSMSTA SETSTORAGESERVER`. Debe especificar `SSL=YES` parámetro para crear el archivo clave de la base de datos en `dsmsta.opt`. Todas las contraseñas se cifran en `dsmsta.opt`.

```
dsmsta setstorageserver myname=storage_agent_name mypa=sta_password
myhla=ip_address servername=server_name serverpa=server_password hla=ip_address lla=ssl_port
ssl=yes
```

2. Cree el certificado de la base de datos de claves y los certificados predeterminados iniciando el agente de almacenamiento.
3. Para el agente de almacenamiento y el servidor, importe los archivos de certificado de entidad emisora de certificados o `cert256.arm` de la otra parte:

```
gsk8capicmd 64 -cert -add -label ip_address -db cert.kdb -stashed
-file cert256.arm
```

Consejo: Utilice la dirección IP como el nombre de la etiqueta.

4. Puede ver los certificados en la base de datos de claves emitiendo el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

5. Reinicie el agente de almacenamiento y el servidor.
6. Establezca la comunicación entre el servidor y el agente de almacenamiento, emitiendo el mandato siguiente:

```
define server sta hla=ip_address lla=port serverpa=password ssl=yes
```

Referencia relacionada:

QUERY SESSION (Consultar sesiones de cliente)

TCPPOINT

TCPADMINPORT

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL

Para proteger los datos que se transmiten entre un cliente y un agente de almacenamiento, configure el cliente para conectarse al agente de almacenamiento mediante el protocolo SSL.

Antes de empezar

Debe tener el certificado y el número de puerto para el agente de almacenamiento.

Acerca de esta tarea

Después de configurar un agente de almacenamiento para aceptar conexiones SSL, configure los clientes para que se conecten al agente de almacenamiento utilizando SSL.

Procedimiento

Para habilitar la comunicación SSL entre los clientes y el agente de almacenamiento, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con la capa de sockets seguros.

Referencia relacionada:

TCPPOINT

TCPADMINPORT

Autenticación de los usuarios de IBM Spectrum Protect mediante un servidor LDAP

En un sistema IBM Spectrum Protect, los usuarios deben autenticarse en el servidor proporcionando un ID de usuario y contraseña. Si su organización utiliza un servidor LDAP (Lightweight Directory Access Protocol) para gestionar los ID de usuario, puede utilizar el servidor LDAP para autenticar los ID de usuario de IBM Spectrum Protect.

Puede utilizar uno de los siguientes métodos para autenticar a los usuarios con un servidor LDAP:

Método preferido para los servidores de IBM Spectrum Protect V7.1.7 y posteriores

Para utilizar este método, que a veces se conoce como *modo integrado*, los ID de usuarios deben registrarse en la base de datos de Active Directory en un servidor LDAP. A continuación, registre los mismos usuarios con el servidor de IBM Spectrum Protect.

Cuando un ID de usuario registrado accede al servidor de IBM Spectrum Protect, se autentica las credenciales en la base de datos de Active Directory.

Para utilizar este método, siga las instrucciones de la sección Autenticación de los usuarios mediante una base de datos de Active Directory.

Método utilizado para los servidores anteriores a V7.1.7, y por los usuarios de IBM® Security Directory Server

Para utilizar este método, los ID de usuario deben estar registrados en una base de datos de Active Directory en un servidor LDAP. De forma alternativa, se pueden registrar los ID de usuario en una base de datos de IBM Security Directory Server

(anteriormente IBM Tivoli Directory Server) de un servidor LDAP. Con este método, no puede utilizar las cuentas de usuario estándar registradas en el servidor LDAP. Debe crear cuentas de usuario separados que estén asociadas a una unidad

organizativa específica. Para utilizar este método, siga las instrucciones de la sección Gestión de contraseñas y procedimientos

de inicio de sesión (V7.1.1).

- Autenticación de los usuarios mediante una base de datos de Active Directory
Puede autenticar a los usuarios de IBM Spectrum Protect mediante una base de datos de Active Directory en un servidor LDAP (Lightweight Directory Access Protocol). Con este método, utilice las cuentas de usuario estándar registradas en el servidor LDAP. Se puede utilizar el mismo ID de usuario para la autenticación en el servidor de IBM Spectrum Protect y en el servidor LDAP.

Réplica de datos de cliente en otro servidor

El hecho de realizar una réplica de los datos de cliente de un servidor de origen en otro servidor ayuda a garantizar que los datos de cliente copiados están disponibles para su recuperación si el servidor de origen resulta dañado. La réplica realiza una copia incremental de los datos del servidor de origen en el servidor de destino para proporcionar capacidad de migración y recuperación.

Acerca de esta tarea

Si se produce un siniestro y el servidor de origen no está disponible temporalmente, los nodos de cliente pueden recuperar los datos del servidor de destino. Si no se puede recuperar el servidor de origen, puede cambiar las configuraciones de los nodos de cliente para almacenar los datos en el servidor de destino. Cuando se produce una parada, el servidor de origen puede migrar los datos automáticamente a un servidor de destino para la recuperación de datos.

Restricción: Un servidor solo puede replicar datos en un servidor de destino.

Puede replicar los datos que se almacenan en cualquier tipo de agrupación de almacenamiento. El tipo de agrupación de almacenamiento puede ser diferente en el servidor de réplica de origen y el servidor de réplica de destino. Puede controlar la réplica por tipo de datos del nodo de cliente:

- Datos de copia de seguridad activos e inactivos juntos o sólo datos de copia de seguridad activos
- Datos de archivado
- Datos migrados al servidor de origen por clientes de IBM Spectrum Protect for Space Management

Cuando replique datos de agrupaciones de almacenamiento de contenedores de directorios, utilice la protección de la agrupación de almacenamiento para mejorar la eficacia del proceso de réplica y para habilitar la reparación de datos. Cuando utilice el Centro de operaciones para configurar las agrupaciones de almacenamiento, las planificaciones de protección se definen automáticamente de modo que se coordinen con la planificación de la réplica.

Procedimiento

1. Compruebe que los servidores sean compatibles y tengan los recursos del sistema necesarios para utilizar con éxito la réplica.

Se necesita una mayor cantidad de núcleos de procesador y memoria. La base de datos y sus registros deben tener el tamaño adecuado para garantizar que las transacciones se pueden completar. Se necesita una red dedicada, con el ancho de banda suficiente como para gestionar los datos que se van a replicar.

- a. Verifique de que los servidores de origen y destino son compatibles para la réplica. Consulte el apartado Compatibilidad de réplica.
- b. Verifique que el servidor tiene los recursos adecuados para obtener un buen rendimiento. Para obtener más información, consulte el apartado Lista de comprobación para la réplica de nodos.

2. Habilite la réplica. Consulte el apartado Habilitación de la réplica de nodo.
3. Planifique la réplica para el servidor de origen. Para obtener información sobre cómo integrar esta planificación en las planificaciones habituales de mantenimiento del servidor, consulte el apartado Definición de planificaciones para actividades de mantenimiento del servidor.
4. Planifique la protección de la agrupación de almacenamiento para todas las agrupaciones de almacenamiento de contenedores de directorios en el servidor de origen. Consulte el apartado Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio.
5. Supervise la réplica mediante el Centro de operaciones. Para obtener más información, consulte el apartado Lista de comprobación de supervisión diaria.

- Compatibilidad de réplica
Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino sean compatibles para la réplica.
- Habilitación de la réplica de nodo
Puede habilitar la réplica de nodo para proteger los datos.
- Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio
Proteja los datos de las agrupaciones de almacenamiento de contenedores de directorio para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedores de directorio.
- Modificación de los valores de réplica
Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.
- Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino
Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

Compatibilidad de réplica

Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino sean compatibles para la réplica.

Tabla 1. Compatibilidad de réplica de versiones de servidor

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V7.1	V7.1 o posterior
V7.1.1	V7.1 o posterior
V7.1.3	V7.1.3 o posterior
V7.1.4	V7.1.3 o posterior
V7.1.5	V7.1.3 o posterior
V7.1.6	V7.1.3 o posterior
V7.1.7	V7.1.3 o posterior
V7.1.8	V7.1.3 o posterior
V8.1	V7.1.3 o posterior
V8.1.1	V7.1.3 o posterior
V8.1.2	V7.1.3 o posterior
V8.1.3	V7.1.3 o posterior

Habilitación de la réplica de nodo

Puede habilitar la réplica de nodo para proteger los datos.

Antes de empezar

Asegúrese de que los servidores de origen y destino son compatibles para la réplica.

Acerca de esta tarea

Replice el nodo de cliente para replicar todos los datos de cliente, incluyendo metadatos. De forma predeterminada, la réplica de nodo está inhabilitada cuando se inicia el servidor por primera vez.

Sugerencias:

- Para reducir el tiempo de proceso de réplica, proteja la agrupación de almacenamiento antes de replicar los nodos de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya se han replicado a través de la protección de agrupación de almacenamiento se omiten.
- La réplica requiere gran cantidad de memoria y ancho de banda suficiente para completar el proceso. Cambie el tamaño de la base de datos y sus registros para garantizar que las transacciones se pueden completar.


Procedimiento

Para habilitar la réplica de nodo, complete los siguientes pasos en Centro de operaciones:

- a. En la página Servidores, pulse Detalles.
- b. En la página Detalles, pulse Propiedades.
- c. En la sección Réplica, seleccione Habilitada en el campo Réplica de salida.
- d. Pulse Guardar.

Qué hacer a continuación

Realice las acciones siguientes:

1. Para verificar que la réplica es correcta, revise el apartado Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Siga las instrucciones del apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio

Proteja los datos de las agrupaciones de almacenamiento de contenedores de directorio para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedores de directorio.

Antes de empezar

Asegúrese de que exista al menos una agrupación de contenedores en directorios en el servidor de réplica de destino. Cuando habilita la réplica en el Centro de operaciones, puede planificar la protección de agrupación de almacenamiento. Para configurar la réplica y habilitar la protección de agrupación de almacenamiento, complete los siguientes pasos:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
2. En la página Réplica, pulse Par de servidores.
3. Complete los pasos del asistente Añadir par de servidores.

Acerca de esta tarea

La protección de una agrupación de almacenamiento de contenedores de directorio hace copias de seguridad de extensiones en otra agrupación de almacenamiento y puede mejorar el rendimiento de la réplica de nodos. Cuando se inicia la réplica de nodo, se omiten las extensiones de datos de las que ya se han hecho copias de seguridad a través de la protección de la agrupación de almacenamiento, lo cual reduce el tiempo de proceso de la réplica. Puede planificar la protección de agrupaciones de almacenamiento varias veces al día para estar al día con los cambios realizados en los datos.

Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor. Debe utilizar agrupaciones de almacenamiento de contenedores de directorios si solo desea proteger y realizar la copia de seguridad de la agrupación de almacenamiento.

Estrategia de protección alternativa: Como alternativa al uso de la réplica, puede proteger los datos en agrupaciones de almacenamiento de contenedores de directorios copiando los datos en las agrupaciones de almacenamiento de copia de contenedor. Los datos de las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta. Las copias de cinta que se almacenan fuera del local proporcionan protección adicional de recuperación ante siniestro en un entorno replicado.

Procedimiento

1. Como alternativa para habilitar la protección de agrupación de almacenamiento, puede utilizar el mandato PROTECT STGPOOL desde el servidor de origen para realizar la copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedores de directorios. Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio denominada POOL1, emita el siguiente mandato:

```
protect stgpool pool1
```

Como parte de la operación del mandato PROTECT STGPOOL, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato AUDIT CONTAINER podría identificar daños en la agrupación de almacenamiento de destino antes de que se emita el mandato PROTECT STGPOOL.

2. Opcional: Si las extensiones dañadas se han reparado en la agrupación de almacenamiento de destino y protege varias agrupaciones de almacenamiento de origen en una agrupación de almacenamiento de destino, siga los pasos siguientes para garantizar una reparación completa:
 - a. Emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen para reparar el máximo daño posible.
 - b. Vuelva a emitir el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen. Para esta segunda operación, utilice el parámetro FORCERECONCILE=YES. Este paso garantiza que las reparaciones de otras agrupaciones de origen se reconocen correctamente para todas las agrupaciones de almacenamiento de origen.


Resultados

Si una agrupación de almacenamiento de contenedores de directorios está protegida, puede reparar la agrupación de almacenamiento si se producen daños mediante el mandato REPAIR STGPOOL.


Restricción: Si replica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorio, no puede reparar la agrupación de almacenamiento.

Qué hacer a continuación


Realice las acciones siguientes:


1. Para ver el estado de la carga de trabajo de la operación de réplica, siga las instrucciones del apartado Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Siga las instrucciones del apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Tareas relacionadas:

 Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta

Referencia relacionada:

 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

 PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)

Modificación de los valores de réplica

Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.

Acerca de esta tarea

Es posible que tenga que personalizar los valores de réplica en los siguientes escenarios:

- Cambios en las prioridades de datos
- Cambios en las reglas de réplica
- Requisito para que otro servidor sea el servidor de destino
- Procesos planificados que afectan de forma negativa al rendimiento de servidor

Procedimiento

Utilice el Centro de operaciones para modificar valores de réplica.

Tarea	Procedimiento
Cambiar una regla de réplica.	<ol style="list-style-type: none">a. En la página Servidores, pulse Detalles.b. En la página Detalles, pulse Propiedades.c. En la sección Réplica, elija la regla de réplica que desea aplicar: Regla de archivado predeterminada, Regla de copia de seguridad predeterminada o Regla de gestión de espacio predeterminada.d. Pulse Guardar.
Especifique el tiempo que se retienen los registros de réplica.	<ol style="list-style-type: none">a. En la página Servidores, pulse Detalles.b. En la página Detalles, pulse Propiedades.c. En la sección Réplica, entre el número de días que deben retenerse los registros de réplica en el campo Retener historial de réplica. Sino, seleccione la casilla de verificación No retener si no necesita registros de réplica.d. Pulse Guardar.
Especifique un servidor de réplica de destino.	<ol style="list-style-type: none">a. En la página Servidores, pulse Detalles.b. En la página Detalles, pulse Propiedades.c. En la sección Réplica, especifique el servidor de destino.d. Pulse Guardar.
Cancele un proceso de réplica.	<ol style="list-style-type: none">a. En la página Servidores, pulse Tareas activas.b. Seleccione el proceso o sección que desea cancelar.c. Pulse Cancelar.

Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino

Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

Procedimiento

1. Desde el servidor de réplica de origen, valide la configuración de la réplica y verifique que el servidor de réplica de origen se puede comunicar con el servidor de réplica de destino mediante el mandato VALIDATE REPLICATION. Por ejemplo, valide la configuración utilizando el nombre de un nodo de cliente que se está replicado:

```
validate replication node1 verifyconnection=yes
```

2. Desde el servidor de réplica de origen, emita el mandato VALIDATE REPLPOLICY para revisar las diferencias entre las políticas en los servidores de réplica de origen y de destino. Por ejemplo, para mostrar las diferencias entre las políticas en el servidor de origen y el servidor de destino, CVT_SRV2, emita el mandato siguiente desde el servidor de origen:

```
validate replpolicy cvt_srv2
```

3. Actualice las políticas en el servidor de destino, si es necesario.

Consejo: Puede utilizar el Centro de operaciones para modificar las políticas en el servidor de destino. Siga las instrucciones de la sección Edición de políticas.

Por ejemplo, para mantener versiones inactivas de archivos durante un periodo de tiempo más corto en el servidor de destino que en el servidor de origen, reduzca el valor de Copias de seguridad en las clases de gestión que se aplican a datos de cliente replicados.

4. Permita al servidor de réplica de destino utilizar sus políticas para gestionar los datos del nodo de cliente replicado emitiendo el mandato SET DISSIMILARPOLICIES en el servidor de origen. Por ejemplo, para habilitar las políticas en el servidor de réplica de destino, CVT_SRV2, emita el mandato siguiente en el servidor de origen:

```
set dissimilarpolicies cvt_srv2 on
```


La próxima vez que se ejecuta el proceso de réplica, se utilizarán las políticas del servidor de réplica de destino para gestionar los datos del nodo del cliente replicado.


Consejo: Si configura la réplica utilizando el Centro de operaciones y las políticas en los servidores de réplica de origen y destino no coinciden, se aplica la política que se ha especificado para el servidor de réplica de origen. Si ha habilitado las políticas en el servidor de réplica de destino utilizando el mandato SET DISSIMILARPOLICIES, se utiliza la política especificada para el servidor de réplica de destino. Si el servidor de réplica de destino no tiene la política que utiliza el nodo en servidor de réplica de origen, se utiliza la política STANDARD.


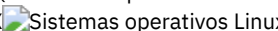

Referencia relacionada:

 EXPORT POLICY (Exportar información de políticas)

 SET DISSIMILARPOLICIES (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)

 VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)

 VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Configuración de entornos en clúster

Puede configurar el servidor de IBM Spectrum Protect para la agrupación en clúster en sistemas AIX, Linux o Windows.

Puede utilizar un entorno de clúster para los siguientes sistemas operativos:




- IBM® PowerHA SystemMirror para AIX
- IBM Tivoli System Automation for Multiplatforms para AIX y Linux
- Microsoft Failover Cluster para Windows

Puede utilizar otros productos de clúster con IBM Spectrum Protect, aunque no hay documentación disponible y el soporte está limitado. Para obtener la información más reciente sobre el soporte para entornos en clúster, consulte <http://www.ibm.com/support/docview.wss?uid=swg21609772>.

Antes de utilizar otro producto de clúster, verifique que DB2 dé soporte a los sistemas de archivos necesarios. Para obtener más información sobre el nivel de DB2 que está utilizando, consulte la Información del producto DB2 y busque los sistemas de archivos recomendados.




- Visión general del entorno en clúster
Los *clústeres* están formados por distintos componentes como, por ejemplo, servidores de IBM Spectrum Protect, hardware y

software. Puede utilizar la agrupación en clúster para unir dos o más servidores o nodos utilizando un subsistema de disco compartido.

-  **Sistemas operativos AIX** Configuración de un entorno de AIX para agrupación en clúster
Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM PowerHA SystemMirror for AIX o IBM Tivoli System Automation for Multiplatforms.
-  **Sistemas operativos Linux** Configuración de un entorno de Linux para agrupación en clúster
Puede configurar el servidor Linux de IBM Spectrum Protect en un entorno en clúster utilizando IBM Tivoli System Automation for Multiplatforms Versión 3.2.2.
-  **Sistemas operativos Windows** Configuración de un entorno en clúster de Windows
Puede configurar un servidor de IBM Spectrum Protect para Windows en un entorno de clúster de migración tras error de Microsoft. Los entornos de clúster de Windows están formados por componentes como, por ejemplo, servidores IBM Spectrum Protect, hardware y software. Si estos componentes están conectados al mismo sistema de disco el tiempo de inactividad se minimiza.

Información relacionada:

Actualización del servidor en un entorno en clúster

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Windows**

Visión general del entorno en clúster

Los *clústeres* están formados por distintos componentes como, por ejemplo, servidores de IBM Spectrum Protect, hardware y software. Puede utilizar la agrupación en clúster para unir dos o más servidores o nodos utilizando un subsistema de disco compartido.

Esta configuración proporciona a los nodos la capacidad de compartir datos, lo que permite una mayor disponibilidad del servidor y minimiza el tiempo de inactividad. Por ejemplo:

- Puede configurar, supervisar y controlar las aplicaciones y los componentes de hardware que se despliegan en un clúster.
- Puede utilizar una interfaz de clúster de administrador y IBM Spectrum Protect para designar organizaciones de clústeres y definir el patrón de recuperación de errores. El servidor forma parte del clúster, lo que proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.
- Puede aplicar la agrupación en clúster al proceso de réplica de nodo. De esta forma, la disponibilidad del servidor es mayor de lo que debería si se utiliza la réplica de nodo como un proceso por sí mismo. La capacidad del servidor es mayor porque es menos probable que un cliente migre tras error a otro servidor en un entorno en clúster. Si replica datos desde varios servidores de réplica fuente a un servidor de réplica de destino, hay una alta dependencia en el servidor de réplica de destino. Un entorno en clúster facilita la dependencia en el servidor de réplica de destino.

Los componentes de un clúster de servidores se denominan *objetos de clúster*. Los objetos de clúster se asocian con un conjunto de propiedades que tienen valores de datos que describen la identidad y el comportamiento de un objeto en el clúster. Los objetos de clúster pueden incluir los componentes siguientes:

- Nodos
- Almacenamiento
- Servicios y aplicaciones
- Redes

Puede gestionar los objetos de clúster mediante la manipulación de sus propiedades, normalmente, a través de una aplicación de gestión de clústeres.

- Nodos de clúster
Los nodos de un clúster tienen características similares, lo que les permite trabajar conjuntamente.

 **Sistemas operativos AIX**











Configuración de un entorno de AIX para agrupación en clúster


Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM® PowerHA SystemMirror for AIX o IBM Tivoli System Automation for Multiplatforms.

PowerHA SystemMirror for AIX y Tivoli System Automation detectan anomalías del sistema y gestionan la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario final. Puede configurar el servidor de IBM Spectrum Protect en un sistema PowerHA o en un clúster de Tivoli System Automation. A continuación, si el sistema falla, el servidor de IBM Spectrum Protect puede iniciarse en otro sistema del clúster.

Tanto en la migración tras error como el restablecimiento, parece que el servidor de IBM Spectrum Protect se detiene y, a continuación, se reinicia. Cualquier transacción que estuviera en curso en el momento del restablecimiento o de la recuperación tras error se retrotrae y todas las transacciones completas siguen estando completas. Los clientes de IBM Spectrum Protect interpretan esto como una anomalía de comunicación e intentan restablecer las conexiones.

Consulte la siguiente información para obtener más detalles sobre estas opciones de agrupación en clúster.

- Configure IBM Spectrum Protect para AIX para utilizar IBM PowerHA SystemMirror for AIX en un entorno en clúster revisando los temas siguientes.
- Configure IBM Spectrum Protect for AIX para utilizar Tivoli System Automation en un entorno de agrupación en clúster revisando la información de <http://www.ibm.com/support/docview.wss?uid=swg27039780>.
- Obtenga más información acerca de Información sobre el producto PowerHA SystemMirror.
-  Sistemas operativos AIX Requisitos de un clúster de PowerHA
IBM PowerHA SystemMirror para AIX detecta los errores del sistema y gestiona la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario.
-  Sistemas operativos AIX Recuperación de errores y restablecimiento de PowerHA
Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.
-  Sistemas operativos AIX Instalación y configuración de PowerHA SystemMirror para AIX
Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM PowerHA tm trademark="SystemMirror" tmtpe="reg">SystemMirror para AIX.
-  Sistemas operativos AIX Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA
Instale el servidor de IBM Spectrum Protect en un nodo de producción para PowerHA para poder configurar el servidor para la agrupación en clúster.
-  Sistemas operativos AIX Instalación del cliente de IBM Spectrum Protect en un nodo de producción para PowerHA
Sólo es necesario instalar el conjunto de archivos del cliente de archivado y copia de seguridad, que contiene los archivos del cliente de archivado y copia de seguridad y el cliente de línea de mandatos administrativos.
-  Sistemas operativos AIX Verificación de la configuración del servidor de IBM Spectrum Protect para PowerHA
Cuando haya configurado el servidor de IBM Spectrum Protect para utilizar PowerHA, debe verificar la configuración.
-  Sistemas operativos AIX Configuración del nodo de espera para PowerHA
Para PowerHA, asegúrese de que el servidor de IBM Spectrum Protect no se esté ejecutando en el nodo de producción antes de configurar el nodo de espera.
-  Sistemas operativos AIX Definición de los dispositivos de almacenamiento de medios extraíbles en AIX para PowerHA
En un sistema operativo AIX, debe definir los dispositivos de almacenamiento de medios extraíbles que utiliza IBM Spectrum Protect en los nodos de producción y espera. El gestor de bibliotecas comprueba que el cartucho que contiene el dispositivo de almacenamiento de soportes extraíble de la unidad está en la unidad correcta.
-  Sistemas operativos AIX Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect
Actualice la configuración del gestor del clúster para definir el servidor de IBM Spectrum Protect como una aplicación y un recurso de recuperación de errores del nodo en espera. Esta aplicación es propiedad del nodo de producción.
-  Sistemas operativos AIX Resolución de problemas del entorno en clúster de PowerHA
Revise la siguiente lista para obtener información sobre la resolución de problemas habituales. La información que se proporciona para IBM PowerHA SystemMirror para AIX no representa todos los casos posibles.

 Sistemas operativos AIX


Requisitos de un clúster de PowerHA

IBM PowerHA SystemMirror para AIX detecta los errores del sistema y gestiona la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario.

Los requisitos de hardware siguientes son para configurar el servidor de IBM Spectrum Protect:

- Una configuración de hardware que sea adecuada para PowerHA. Los dispositivos de almacenamiento de medios extraíbles del servidor de IBM Spectrum Protect deben estar conectados físicamente a al menos dos nodos del clúster de PowerHA en un bus compartido (incluida una SAN).
- Suficiente espacio de disco compartido para contener la base de datos de IBM Spectrum Protect, las anotaciones de recuperación, el directorio de instancia y las agrupaciones de almacenamiento de disco que se van a utilizar. Consulte Gestión de la capacidad de inventario para determinar cuánto espacio se requiere para el registro de base de datos y recuperación, y para garantizar la disponibilidad del registro de base de datos y recuperación.
- Una red TCP/IP.

Consejo: Si un servidor de IBM Spectrum Protect gestiona dispositivos de almacenamiento de medios extraíbles, puede configurar dos servidores de IBM Spectrum Protect para que se ejecuten en sistemas diferentes en un clúster de PowerHA. Cada sistema puede ejecutar ambos servidores si el otro sistema falla. Para configurar dos servidores de IBM Spectrum Protect para que se ejecuten en sistemas diferentes en un clúster de PowerHA, utilice otro sistema de archivos que sea accesible para ambos servidores.

 Sistemas operativos AIX

Recuperación de errores y restablecimiento de PowerHA

Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.

Los términos *nodo de producción* y *nodo de espera* hacen referencia a los dos nodos PowerHA en los que se ejecuta el servidor de IBM Spectrum Protect.


PowerHA gestiona el control de la dirección TCP/IP y el montaje del sistema de archivos compartidos en el nodo de espera o el nodo de producción, según corresponda.

Cuando se produce una *migración tras error* o *restablecimiento*, se retrotraen todas las transacciones que se estaban procesando en ese momento. Para los clientes de IBM Spectrum Protect, la *migración tras error* o el *restablecimiento* representan un error en las comunicaciones. Por lo tanto, debe restablecer una conexión basada en los valores de las opciones COMMRESTARTDURATION y COMMRESTARTINTERVAL.

Por lo general, puede reiniciar el cliente de copia de seguridad/archivado desde la última transacción validada. Si se está ejecutando una planificación de cliente cuando se produce la *migración tras error*, es probable que la operación del cliente falle. Si puede reiniciar las operaciones de cliente, debe reiniciarlas desde el inicio del proceso. Las operaciones de clientes y de agente se completan como hacen normalmente si el servidor se ha detenido y reiniciado mientras estaban conectadas. La única diferencia es que el servidor se reinicia físicamente en un hardware diferente.

Si no desea que se produzca un *restablecimiento* automático, puede configurar el recurso como un grupo de recursos en cascada sin *restablecimiento*.


Información relacionada:

 Información sobre el producto PowerHA SystemMirror

Instalación y configuración de PowerHA SystemMirror para AIX

Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM® PowerHA tm trademark="SystemMirror" tmttype="reg">SystemMirror para AIX.

-  Sistemas operativos AIX Instalación y configuración del clúster de PowerHA
Puede experimentar errores de proceso si la instalación y la configuración de IBM PowerHA SystemMirror para AIX no se realizan correctamente.
-  Sistemas operativos AIX Configuración del servidor de IBM Spectrum Protect en el nodo primario para PowerHA
Puede configurar una instancia de servidor IBM Spectrum Protect en el nodo primario.
-  Sistemas operativos AIX Configuración de servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia compartida de DB2
Si el directorio de instancia de DB2 se comparte entre los nodos del clúster de PowerHA, no necesita crear una instancia de DB2 en el nodo secundario. No ejecute el asistente dsmicfgx.
-  Sistemas operativos AIX Configuración del servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia de DB2 separada
Debe crear una instancia de DB2 en cada nodo secundario si el directorio de instancia de DB2, /home/tsminst1/sqllib, no está compartido entre los nodos en el clúster de PowerHA.

 Sistemas operativos AIX

Instalación y configuración del clúster de PowerHA

Puede experimentar errores de proceso si la instalación y la configuración de IBM PowerHA SystemMirror para AIX no se realizan correctamente.


Procedimiento

Siga estos pasos para instalar y configurar el clúster de PowerHA:

1. Defina los sistemas de archivos compartidos y los volúmenes lógicos, cuando sea necesario. Si lo desea, puede colocar los archivos en sistemas de archivos independientes o en discos físicos independientes por motivos de integridad o rendimiento. No ponga el directorio de inicio de la instancia de usuario en un disco compartido. Duplique los volúmenes lógicos para ofrecer la máxima disponibilidad (incluidos los sistemas de archivos subyacentes). Los sistemas de archivos que deben definirse incluyen el directorio de instancia de servidor de IBM Spectrum Protect, los directorios de registro y de base de datos, todos los directorios de agrupación de almacenamiento de disco y los directorios de agrupación de almacenamiento de tipo de dispositivo FILE.
2. Configure PowerHA para que el nodo de producción sea el propietario de los grupos de volúmenes compartidos y el nodo en espera se encargue de los grupos de volúmenes compartidos si el nodo de producción falla.
3. Configure PowerHA para la recuperación de errores de los sistemas de archivos.
4. Configure una dirección IP de servicio para el servidor de IBM Spectrum Protect. La dirección IP de servicio debe ser distinta de la dirección IP de cada host. La IP de servicio se mueve de un host a otro, no la dirección IP de host real.
5. Realice la recuperación de errores de la base de datos compartida y los directorios de anotaciones y de instancias en el nodo en espera del clúster de PowerHA.

Resultados

Debe configurar los dispositivos de almacenamiento de medios extraíbles para la recuperación de errores y definir el servidor de IBM Spectrum Protect como una aplicación en PowerHA.

 Sistemas operativos AIX

Configuración del servidor de IBM Spectrum Protect en el nodo primario para PowerHA


Puede configurar una instancia de servidor IBM Spectrum Protect en el nodo primario.

Procedimiento

1. Revise los temas en la información de configuración del servidor de IBM Spectrum Protect.
2. Después de configurar la instancia del servidor de IBM Spectrum Protect en el nodo primario, puede configurar el servidor de IBM Spectrum Protect en un nodo secundario.

Tareas relacionadas:

Configuración de la instancia del servidor de IBM Spectrum Protect

 Sistemas operativos AIX

Configuración de servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia compartida de DB2

Si el directorio de instancia de DB2 se comparte entre los nodos del clúster de PowerHA, no necesita crear una instancia de DB2 en el nodo secundario. No ejecute el asistente dsmsicfgx.

Procedimiento

Para configurar una instancia de servidor en el nodo secundario con una instancia de DB2 compartida, siga los siguientes pasos:

1. En cada nodo del clúster, añada el siguiente texto para el script `/opt/tivoli/tsm/server/bin/rc.dsmserv`:

```
DB2NODES_TEMP='/tmp/db2nodes.tmp'
DB2NODES=${homeDir}/sqllib/db2nodes.cfg
# Current hostname
HOSTNAME=$(/bin/hostname)
# hostname saved in db2nodes.cfg
DB2_HOST=$(cat $DB2NODES | cut -d ' ' -f 2)
# if they are different update the file
if [[ "$HOSTNAME" != "$DB2_HOST" ]]
then
  echo "Updating hostname in db2nodes.cfg"
  sed -e s_${DB2_HOST}_${HOSTNAME}_g $DB2NODES > $DB2NODES_TEMP
  cp $DB2NODES_TEMP $DB2NODES
fi
```

Consejo: Si el texto no se incluye en el script puede incluirlo antes de emitir mandatos de `/opt/tivoli/tsm/server/bin/rc.dsmserv`.

- Traslade todos los recursos compartidos al nodo secundario.
- Actualice las siguientes variables en el script `/opt/tivoli/tsm/server/bin/startserver`, utilizando los siguientes valores:

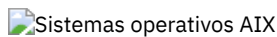
Tabla 1. Variables en el script `/opt/tivoli/tsm/server/bin/startserver`

Descripción	Variabl e	Ejemplo
Defina INST_USER en el ID de usuario de instancia.	INST_U SER	INST_USER='tsmuser1'
Defina INST_DIR como la ubicación del directorio de instancia de IBM Spectrum Protect. Este directorio contiene dsmserv.dbid y dsmserv.opt.	INST_DI R	INST_DIR='/home/tsmu ser1/tsminst1'
Seleccione una de las siguientes opciones de inicio: Opción 1: utilice la instancia \$INST_USER pero ejecute el servidor como raíz (-U) Opción 2: utilice la instancia \$INST_USER y ejecute el servidor como \$INST_USER (-u)	INST_O PTION	Opción 1: INST_OPTION='-U \$INST_USER' Opción 2: INST_OPTION='-u \$INST_USER'

- Inicie el servidor emitiendo el script siguiente:

```
/opt/tivoli/tsm/server/bin/startserver
```

- Cuando se inicie el servidor, emita el mandato BACKUP DB para verificar que se ha realizado la copia de seguridad de los datos correctamente.



Sistemas operativos AIX

Configuración del servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia de DB2 separada

Debe crear una instancia de DB2 en cada nodo secundario si el directorio de instancia de DB2, `/home/tsminst1/sqllib`, no está compartido entre los nodos en el clúster de PowerHA.

Acerca de esta tarea

Puede configurar el servidor de IBM Spectrum Protect en un nodo secundario utilizando el asistente de `dsmicfgx` o de forma manual.

Procedimiento

- Para crear una instancia de DB2 en un nodo secundario utilizando el asistente de `dsmicfgx`, siga estos pasos:
 - Ejecute el asistente de `dsmicfgx`.
 - Desde el panel de Directorio de instancia, seleccione la casilla de verificación **Seleccionar esto si está configurando la instancia del servidor en un nodo secundario de un clúster de alta disponibilidad**.
- Para crear una instancia de DB2 en un nodo secundario de forma manual, siga estos pasos:
 - Traslade todos los recursos compartidos al nodo secundario.
 - Cree una instancia de DB2 emitiendo el siguiente mandato `db2icrt`:

```
/opt/tivoli/tsm/db2/instance/db2icrt -s ese -u instance_user instance_user
```

donde `instance_user` es el mismo usuario que posee la instancia de DB2 en el nodo primario.

- Cuando se cree la instancia de DB2, inicie sesión como el usuario de la instancia o emita el mandato su:

```
su - <instance_user>
```

- Como usuario de instancia, emita los siguientes mandatos:

```
db2start
db2 update dbm cfg using DFTDBPATH shared_db_path
db2 catalog db TSMDB1
db2stop
```

donde `shared_db_path` es el directorio de base de datos compartido. El directorio de base de datos compartidos es normalmente el directorio de instancia del servidor.

Consejo: Para determinar el valor `shared_db_path`, emita el siguiente mandato en el nodo primario:

```
db2 get dbm cfg | grep DFTDBPATH
```

5. Actualice las siguientes variables en el script `/opt/tivoli/tsm/server/bin/startserver`, utilizando los siguientes valores:


Tabla 1. Variables en el script `/opt/tivoli/tsm/server/bin/startserver`

Descripción	Variabl e	Ejemplo
Defina INST_USER en el ID de usuario de instancia.	INST_U SER	INST_USER='tsmuser1' '
Defina INST_DIR como la ubicación del directorio de instancia de IBM Spectrum Protect. Este directorio contiene dsmserv.dbid y dsmserv.opt.	INST_D IR	INST_DIR='/home/tsm user1/tsminst1'
Seleccione una de las siguientes opciones de inicio: Opción 1: utilice la instancia \$INST_USER pero ejecute el servidor como raíz (-U) Opción 2: utilice la instancia \$INST_USER y ejecute el servidor como \$INST_USER (-u)	INST_O PTION	Opción 1: INST_OPTION='-U \$INST_USER' Opción 2: INST_OPTION='-u \$INST_USER'

6. Inicie el servidor emitiendo el script siguiente:

```
/opt/tivoli/tsm/server/bin/startserver
```

7. Cuando se inicie el servidor, emita el mandato BACKUP DB para verificar que se ha realizado la copia de seguridad de los datos correctamente.

 Sistemas operativos AIX

Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA

Instale el servidor de IBM Spectrum Protect en un nodo de producción para PowerHA para poder configurar el servidor para la agrupación en clúster.

Procedimiento

Complete los pasos siguientes para instalar el servidor de IBM Spectrum Protect en el nodo de producción:

1. Instale IBM Spectrum Protect. Seleccione uno de los siguientes componentes:
 - El servidor de IBM Spectrum Protect
 - El controlador de dispositivo de IBM Spectrum Protect, si es necesario
 - La licencia de IBM Spectrum Protect

Los archivos ejecutables se instalan normalmente en los discos internos del nodo de producción, no en el espacio de discos de IBM Spectrum Protect compartido. Los archivos ejecutables del servidor de IBM Spectrum Protect se instalan en el directorio `/opt/tivoli/tsm/server/bin`.

2. Configure IBM Spectrum Protect para utilizar el método de comunicación TCP/IP. Para obtener instrucciones, consulte la información sobre la configuración de una instancia de servidor en AIX: Realización de los primeros pasos después de instalar IBM Spectrum Protect.
3. Defina un nuevo ID de usuario para que sea el propietario de la instancia de servidor de IBM Spectrum Protect o utilice un ID de usuario existente que aún no sea propietario de una instancia de IBM Spectrum Protect. Con la sesión iniciada con el ID de usuario de la instancia, siga estos pasos:
 - a. Crear un directorio de instancia utilizando el mandato `mkdir` en un sistema de archivos compartidos que puede migrar tras error al sistema en espera. Este disco debe definirse en PowerHA.
 - b. Crear la base de datos y directorios de registro mediante la utilización del mandato `mkdir` en sistemas de archivos compartidos que se puedan migrar tras error al sistema en espera. Estos discos también deben definirse en PowerHA para la recuperación de errores.
 - c. Complete la configuración utilizando el asistente `dsmicfgx`.

Tareas relacionadas:

AIX: Instalación del servidor
Actualización del servidor

Instalación del cliente de IBM Spectrum Protect en un nodo de producción para PowerHA

Sólo es necesario instalar el conjunto de archivos del cliente de archivado y copia de seguridad, que contiene los archivos del cliente de archivado y copia de seguridad y el cliente de línea de mandatos administrativos.

Procedimiento

Para obtener instrucciones detalladas sobre la instalación del cliente de IBM Spectrum Protect, consulte la publicación Instalación de los clientes de copia de seguridad y archivado de IBM Spectrum Protect.

Complete los pasos siguientes para instalar el cliente de IBM Spectrum Protect en el nodo de producción.

1. Instale los archivos ejecutables del cliente de IBM Spectrum Protect en el directorio `/usr/tivoli/tsm/client/ba/bin`. Estos archivos se instalan normalmente en los discos internos del nodo de producción.
2. Para que el cliente encuentre el servidor, asegúrese de que el archivo de opciones de cliente, `dsm.sys`, apunte al servidor de IBM Spectrum Protect. El nombre de servidor `dsm.sys` se utiliza sólo en el parámetro `-servername` del mandato `dsmadm` para especificar el servidor al que se va a conectar.

Verificación de la configuración del servidor de IBM Spectrum Protect para PowerHA

Cuando haya configurado el servidor de IBM Spectrum Protect para utilizar PowerHA, debe verificar la configuración.

Acerca de esta tarea

Cuando utiliza PowerHA, todos los directorios de base de datos, anotaciones, almacenamiento e instancia deben estar en discos compartidos que estén configurados para que PowerHA pueda ejecutar la recuperación de errores.

Procedimiento

Para identificar los directorios que están en el disco compartido, siga estos pasos:

1. Inicie una sesión como el usuario de instancia.
2. Ejecute el script `/opt/tivoli/tsm/server/bin/dsmclustfs`.
3. Examine los sistemas de archivos que recoge el script y compruebe que estén en discos compartidos. El siguiente script de ejemplo muestra el tipo de información que debe revisar:

```
> su - tsminst1
$ /opt/tivoli/tsm/server/bin/dsmclustfs
SQL1026N El gestor de base de datos ya está activo.
```

La siguiente información sobre conexión de base de datos se muestra cuando el servidor de IBM Spectrum Protect se conecta a la base de datos de DB2:

```
DB20000I El mandato START DATABASE MANAGER se ha ejecutado correctamente.
```

```
Database Connection Information
```


```
Database server          = DB2/AIX64 11.1.0
SQL authorization ID     = TSMINST1
Local database alias     = TSMDB1
```

```
File systems for the DB2 database: /TSMdbspace2 /TSMdbspace1
File system for Active Log: /TSMalog
File system for Archive Log: /TSMarchlog
Active log mirror not defined for this database
```

Los siguientes sistemas de archivos de DB2 obligatorios están en el script:

```
/TSMdb-1 /TSMalog-1 /TSMarchlog-1
```

Checking existing TSM disk-based volumes...
TSM Data is stored in the following file systems: /TSMdisk-1 /TSMfile-1

 Sistemas operativos AIX

Configuración del nodo de espera para PowerHA

Para PowerHA, asegúrese de que el servidor de IBM Spectrum Protect no se esté ejecutando en el nodo de producción antes de configurar el nodo de espera.


Procedimiento

Complete los pasos siguientes para configurar el nodo de espera:

1. En el nodo de espera, abra el grupo de volúmenes compartidos y los sistemas de archivos de IBM Spectrum Protect.
2. En el nodo de espera, instale el código de producto de IBM Spectrum Protect. Para obtener más información, consulte el apartado Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA. Si los archivos ejecutables se instalan en un espacio de disco compartido, es posible que deba instalarlos en el nodo en espera. Los controladores de dispositivo de IBM Spectrum Protect, los paneles SMIT y otros archivos deben instalarse en directorios del sistema AIX.
3. Abra el asistente dsmicfgx. Siga las instrucciones para completar la configuración. Seleccione el recuadro de selección para indicar que se trata de un nodo secundario del clúster.
4. Inicie el servidor en el nodo de espera. Consulte la base de datos, las anotaciones de recuperación y los volúmenes de agrupaciones de almacenamiento para comprobar que son los mismos que cuando se inició el servidor en el nodo de producción.
5. Instale el cliente en el nodo de espera. Si los archivos ejecutables se instalan en un espacio de disco compartido, es posible que deba instalarlos en el nodo en espera. Los paneles SMIT de IBM Spectrum Protect y otros archivos deben instalarse en directorios del sistema AIX. Utilice el mandato RCP de AIX con la opción -p para copiar el archivo dsm.sys del nodo de producción al nodo en espera. Si el archivo dsm.sys se cambia en un nodo, debe copiarse en el otro.

Resultados

Consejo: Si el archivo dsm.sys se cambia en un nodo, debe copiarlo en el otro.

 Sistemas operativos AIX

Definición de los dispositivos de almacenamiento de medios extraíbles en AIX para PowerHA

En un sistema operativo AIX, debe definir los dispositivos de almacenamiento de medios extraíbles que utiliza IBM Spectrum Protect en los nodos de producción y espera. El gestor de bibliotecas comprueba que el cartucho que contiene el dispositivo de almacenamiento de soportes extraíble de la unidad está en la unidad correcta.

Acerca de esta tarea

Requisito previo:

- Si define un servidor de gestor de bibliotecas que no se comparte con el servidor de IBM Spectrum Protect, asegúrese de que el parámetro RESETDRIVES del mandato DEFINE LIBRARY o el mandato UPDATE LIBRARY esté especificado como YES. Si define un servidor de gestor de bibliotecas que no se comparte con el servidor de IBM Spectrum Protect, la opción SANDISCOVERY debe establecerse en ON en el archivo de opciones de servidor de IBM Spectrum Protect dsmserv.opt. De forma predeterminada, esta opción está establecida en OFF.
- Puede emitir el mandato PERFORM LIBACTION desde los tipos de biblioteca SCSI y VTL. Utilice este mandato para definir las unidades y sus vías de acceso para una biblioteca en un paso.

Si su correlación de dispositivos SAN es precisa, continúe con la sección Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect. Si los nombres de dispositivo de los sistemas primario y secundario no son los mismos, debe utilizar el descubrimiento SAN para que el servidor de IBM Spectrum Protect pueda acceder a los dispositivos.

Tareas relacionadas:

 Configuración del intercambio de biblioteca (V7.1.1)



Referencia relacionada:

DEFINE LIBRARY (Definir una biblioteca)

UPDATE LIBRARY (Actualizar una biblioteca)

PERFORM LIBACTION (Definir o suprimir todas las unidades y vías de acceso de una biblioteca)

Información relacionada:

-  [Dispositivos admitidos de IBM Spectrum Protect](#)
-  [Sistemas operativos AIX](#)




Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect

Actualice la configuración del gestor del clúster para definir el servidor de IBM Spectrum Protect como una aplicación y un recurso de recuperación de errores del nodo en espera. Esta aplicación es propiedad del nodo de producción.

Acerca de esta tarea

Puede emitir mandatos de IBM® PowerHA SystemMirror for AIX o Tivoli System Automation para configurar el clúster. Continúe con la configuración del servidor de IBM Spectrum Protect.

Información relacionada:

-  [Información sobre el producto PowerHA SystemMirror](#)
-  [Información sobre el producto IBM Tivoli System Automation for Multiplatforms versión 3.2.2](#)
-  [Sistemas operativos AIX](#)

Resolución de problemas del entorno en clúster de PowerHA

Revise la siguiente lista para obtener información sobre la resolución de problemas habituales. La información que se proporciona para IBM® PowerHA SystemMirror para AIX no representa todos los casos posibles.

Mensajes de aviso que se emiten después de ejecutar el programa de utilidad clverify

Puede ejecutar el programa de utilidad de verificación de clúster de PowerHA, clverify, en un nodo para verificar la configuración del clúster y la asignación de los recursos de PowerHA. Si ejecuta el programa de utilidad clverify después de definir el servidor de IBM Spectrum Protect como una aplicación PowerHA, aparecerán mensajes de aviso.

Los mensajes de aviso aparecen porque los scripts de shell que inician y detienen los servidores de IBM Spectrum Protect están en un sistema de archivos compartidos. Los scripts de shell sólo pueden ejecutarse en un nodo cada vez. Por lo tanto, los scripts de shell estarán disponibles en sólo un nodo cada vez. Puede ignorar los mensajes de aviso del programa de utilidad clverify. Si un sistema de archivos compartidos no se puede montar, el servidor de IBM Spectrum Protect no puede iniciarse.

El servidor de IBM Spectrum Protect falla al iniciarse una vez emitido el script startserver

Si utiliza el script de shell startserver y PowerHA falla al iniciar el servidor de IBM Spectrum Protect, inícielo de forma manual en un terminal sin la opción quiet. Si desea ejecutar el servidor con la opción QUIET, emita el mandato dsmserv -q.

Mensajes asociados al mandato tctl

Si emite el mandato tctl -f/dev/rmt2 rewind, es posible que aparezca el siguiente mensaje:

```
/dev/rmt2: Ya hay un dispositivo montado o no se puede desmontar
```

Este mensaje indica que un sistema distinto del sistema donde se ha ejecutado el mandato tctl ha bloqueado con SCSI RESERVE el dispositivo E/S. Si utiliza la reserva persistente, el servidor de IBM Spectrum Protect anticipa una reserva de unidad de forma predeterminada. Si el controlador de dispositivo no utiliza la reserva persistente, el servidor completa un restablecimiento de destino.


Mensaje ANS4329S Server out of data storage space

Si aparece el mensaje ANS4329S Server out of data storage space en el cliente de IBM Spectrum Protect, puede que la licencia del servidor de IBM Spectrum Protect no sea válida. Emita el mandato QUERY LICENSE para mostrar la información de conformidad con la licencia. Si el estado de cumplimiento es válido, utilice el mandato QUERY ACTLOG en el servidor y revise los mensajes que se muestran para identificar el problema.

 [Sistemas operativos Linux](#)

Configuración de un entorno de Linux para agrupación en clúster

Puede configurar el servidor Linux de IBM Spectrum Protect en un entorno en clúster utilizando IBM® Tivoli System Automation for Multiplatforms Versión 3.2.2.

-  [Sistemas operativos Linux](#) Descripción general de un clúster de IBM Spectrum Protect de dos nodos utilizando Tivoli System Automation

Utilice el clúster de Tivoli System Automation para una disponibilidad de base de datos y servidor mayor durante un fallo. Mediante la función de migración tras error de Tivoli System Automation, los componentes de servidor como la base de datos se pueden recuperar automáticamente de una anomalía.

-  Sistemas operativos Linux Configuración de un clúster de IBM Spectrum Protect con Tivoli System Automation
Debe configurar un clúster de IBM Spectrum Protect para utilizar Tivoli System Automation.
-  Sistemas operativos Linux Requisitos previos para configurar un entorno en clúster de Linux con Tivoli System Automation
Antes de instalar y configurar IBM Spectrum Protect en un entorno en clúster con Tivoli System Automation, debe comprobar los requisitos previos.
-  Sistemas operativos Linux Instalación y configuración de componentes de IBM Spectrum Protect en los nodos primario y secundario
Debe instalar los componentes de base de datos y servidor de IBM Spectrum Protect en los nodos primario y secundario del clúster. A continuación, configure primero el nodo primario seguido del nodo secundario.
-  Sistemas operativos Linux Instalación de Tivoli System Automation en nodos primario y secundario
Después de instalar y configurar IBM Spectrum Protect en los nodos primario y secundario del clúster, debe instalar y configurar Tivoli System Automation en esos nodos. A continuación, debe activar esos nodos para el dominio, configurar los recursos y activar la política base. Finalmente, debe añadir los puntos de montaje para los directorios de IBM Spectrum Protect.
-  Sistemas operativos Linux Configuración de recursos de almacenamiento
Utilice la interfaz de usuario de Tivoli System Automation o de la línea de mandatos para añadir o suprimir los recursos de almacenamiento y para suprimir los puntos de montaje que ya no son necesarios. Si añade una agrupación de almacenamiento al clúster, debe añadirla al grupo de recursos. Si elimina una agrupación de almacenamiento del clúster, también debe suprimirla del grupo de recursos.
-  Sistemas operativos Linux Actualización de un servidor configurado con Tivoli System Automation
Puede actualizar un servidor configurado con Tivoli System Automation desde la Versión 6.3 o la Versión 7.1.

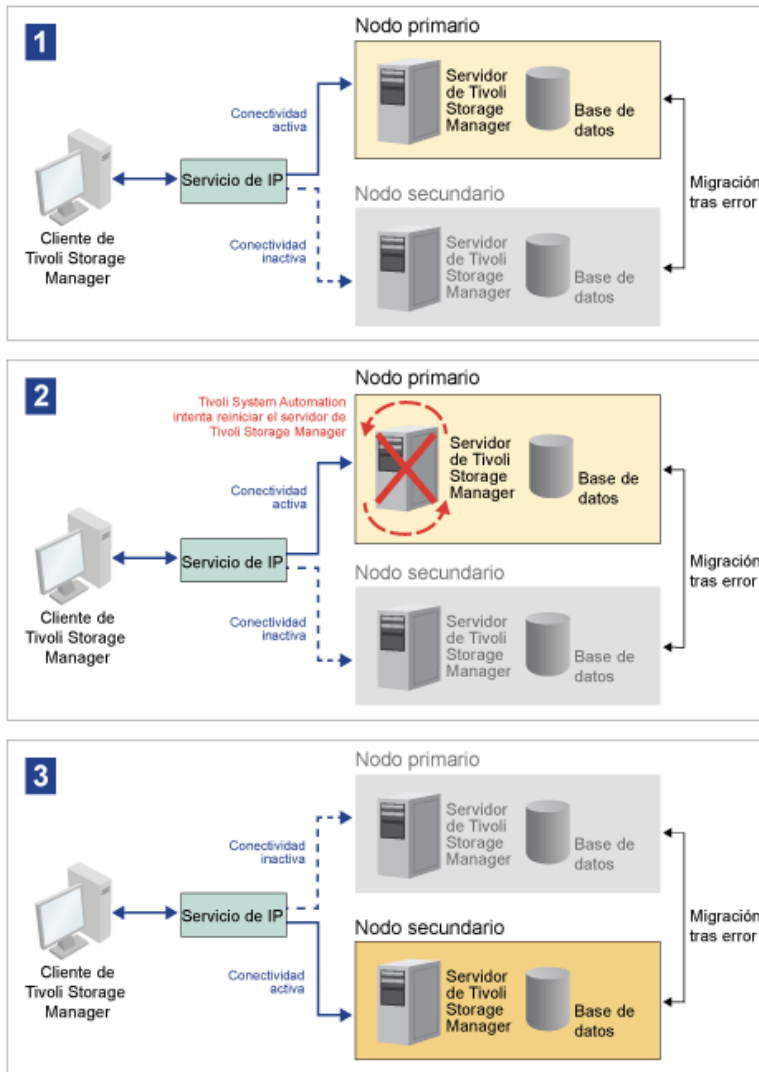
 Sistemas operativos Linux

Descripción general de un clúster de IBM Spectrum Protect de dos nodos utilizando Tivoli System Automation

Utilice el clúster de Tivoli System Automation para una disponibilidad de base de datos y servidor mayor durante un fallo. Mediante la función de migración tras error de Tivoli System Automation, los componentes de servidor como la base de datos se pueden recuperar automáticamente de una anomalía.

El servidor de IBM Spectrum Protect y la base de datos DB2 son componentes de servidor subyacentes para este clúster de dos nodos. El servidor es un componente principal. Es responsable de la actividad del servidor y del cliente. La base de datos DB2 es un componente interno que se instala como parte del servidor. El servidor controla toda actividad de la base de datos como el inicio y el cierre. Cuando el servidor detecta un error de componente de base de datos o de servidor, intenta reiniciar la base de datos. Si el reinicio falla, el servidor y la base de datos se cierran automáticamente en el nodo primario y Tivoli System Automation inicia estos componentes en el nodo secundario. Debido a que las funciones de IBM Spectrum Protect se restauran inmediatamente, la disponibilidad del servidor y de la base de datos es mayor.

Figura 1. Función de migración tras error. Los componentes de servidor y de base de datos falla en el nodo primario. Tivoli System Automation inicia estos componentes en el nodo secundario.

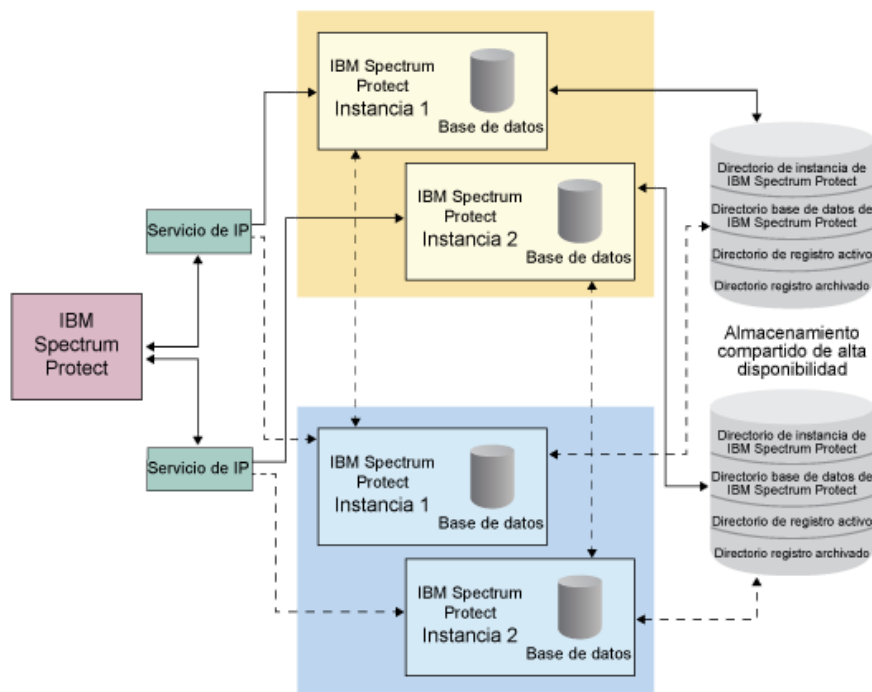


El servidor y la base de datos incluyen los siguientes directorios de registros que se utilizan para el almacenamiento:

- Directorio de instancia de IBM Spectrum Protect
- Directorio de anotaciones activas
- Directorio de anotaciones de archivado
- Directorio de base de datos

Los dos nodos de este clúster de Tivoli System Automation están configurados para acceder a un almacenamiento compartido altamente disponible que protege los datos. Por ejemplo, la topología de dos nodos incluye un nodo primario y un nodo secundario. Estos nodos se ubican en sistemas físicos individuales pero pueden acceder a los mismos datos utilizando la matriz de almacenamiento compartido.

Figura 2. Varias instancias de servidor de IBM Spectrum Protect en nodos separados. Estas instancias de servidor están en sistemas físicos separados. Estas instancias pueden acceder al almacenamiento compartido altamente disponible.



- Sistemas operativos Linux Topología de disco compartido de dos nodos
 Este clúster utiliza una tipología de disco compartido de dos nodos. Incluye un nodo primario y secundario. El nodo primario aloja el servidor de IBM Spectrum Protect, la base de datos, la instancia de IBM Spectrum Protect y los datos. El nodo secundario es adonde se mueven los recursos de IBM Spectrum Protect si se produce un fallo.
- Sistemas operativos Linux Grupos de recursos de Tivoli System Automation
 Utilice los grupos de recursos de Tivoli System Automation con políticas de automatización definidas para gestionar los componentes de IBM Spectrum Protect para este clúster. La única excepción es el recurso de instancia de servidor de base de datos gestionada por el servidor de IBM Spectrum Protect.

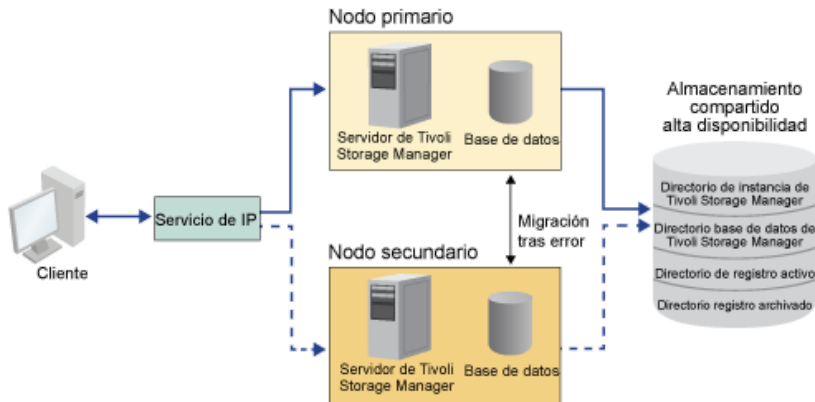
Sistemas operativos Linux

Topología de disco compartido de dos nodos

Este clúster utiliza una tipología de disco compartido de dos nodos. Incluye un nodo primario y secundario. El nodo primario aloja el servidor de IBM Spectrum Protect, la base de datos, la instancia de IBM Spectrum Protect y los datos. El nodo secundario es adonde se mueven los recursos de IBM Spectrum Protect si se produce un fallo.

Los dos nodos de este clúster se conectan uno a otro a través de una única red pública y a un sistema de *almacenamiento de disco compartido*, que siempre está disponible. El *almacenamiento de disco compartido* es donde están disponibles uno o más discos para

los nodos primario y secundario. Estos discos sólo se montan en un nodo, el nodo primario, a la vez. Un nodo puede tener datos de entrada y de salida que se comparten con los discos de almacenamiento. La siguiente ilustración muestra una topología compartida de dos nodos donde se produce una migración tras error automática al nodo secundario en la instancia de un fallo.



 Sistemas operativos Linux

Grupos de recursos de Tivoli System Automation

Utilice los grupos de recursos de Tivoli System Automation con políticas de automatización definidas para gestionar los componentes de IBM Spectrum Protect para este clúster. La única excepción es el recurso de instancia de servidor de base de datos gestionada por el servidor de IBM Spectrum Protect.

Los sistemas de archivo compartido y los componentes de IBM Spectrum Protect se definen como recursos. Varios recursos crean un grupo de recursos. Cada recurso del grupo de recursos tiene un tipo de recurso. Cada instancia de IBM Spectrum Protect de un clúster incluye un grupo de recursos. Durante las paradas planificadas, los grupos de recursos se pueden mover manualmente del nodo primario al nodo secundario.

El grupo de recursos de IBM Spectrum Protect incluye los siguientes recursos. El nombre del grupo de recursos de IBM Spectrum Protect es SA-tsm-inst1-rg, donde inst1 es el nombre de instancia. Los recursos siguientes se utilizan para funciones distintas pero obligatorias en este clúster.

IP de servicio

El recurso de IP de servicio se utiliza para la comunicación. Se denomina tsm-inst1-ip-rs, donde inst1 es el nombre de instancia. La IP de servicio está gestionada por Tivoli System Automation. Esta IP está disponible en el nodo donde se está ejecutando el servidor de IBM Spectrum Protect. Debe crear la interfaz lógica de la IP de servicio en la misma interfaz física que la interfaz de red pública.

Recurso *almacenamiento de disco compartido*

Un recurso de *almacenamiento de disco compartido* es un dispositivo de almacenamiento físico en el servidor de IBM Spectrum Protect donde están almacenados los datos de aplicación de IBM Spectrum Protect y DB2. Debe crear los siguientes recursos de almacenamiento de disco:

- Directorio de instancia - tsm-inst1-instdir-ag
- Directorio de DB2 - tsm-inst1-db2dir-ag
- Directorio de registros activos - tsm-inst1-actlog-ag
- Directorio de registro de archivado - tsm-inst1-archlog-ag

Almacenamiento de disco compartido para agrupaciones de almacenamiento

El recurso de agrupación de almacenamiento incluye dispositivos de almacenamiento físico en el servidor de IBM Spectrum Protect donde se almacenan los datos de cliente.

Recursos del grupo de volúmenes


Si decide configurar el almacenamiento utilizando grupos de volúmenes, hay un recurso de grupo de volúmenes disponible para los recursos de *almacenamiento de disco compartido* anteriores. Los recursos del grupo de volúmenes se crean automáticamente mediante Tivoli System Automation.


Recursos de aplicación para la instancia de servidor de IBM Spectrum Protect

El recurso de instancia de servidor de IBM Spectrum Protect es el recurso de servidor que gestiona la aplicación de IBM Spectrum Protect. Este recurso se gestiona a través de scripts de control de Tivoli System Automation.

Tabla 1. Tareas completadas por los scripts de control de Tivoli System Automation

Tareas	Descripción	Mandatos de ejemplo
START	Inicia la instancia de servidor de IBM Spectrum Protect.	El mandato <code>/opt/tivoli/tsm/server/bin/rc.dsmserv -u db2inst1 -i /tsminst1</code> inicia la instancia de servidor con el usuario db2inst1 del directorio /tsminst1.
Detener	Detiene la instancia de servidor de IBM Spectrum Protect.	<code>kill -s SIGURG 345</code> donde 345 es el <i>PID</i> . El <i>PID</i> se puede encontrar en el archivo <code>/tsminst1/dsmserv.v6lock</code> .
Monitor	Comprueba si existe el archivo <code>/tsminst1/dsmserv.v6lock</code> . Utiliza el <i>PID</i> para comprobar si se está ejecutando el proceso.	<code>ps -ef grep 345</code> donde 345 es el <i>PID</i> .

-  Sistemas operativos Linux Dependencias del grupo de recursos
Las dependencias del grupo de recursos se crean automáticamente para controlar el orden en el que se inician los recursos. Estas dependencias también controlan qué recursos se deben reiniciar o concluir si falla el recurso específico del que dependen estos recursos.

 Sistemas operativos Linux

Configuración de un clúster de IBM Spectrum Protect con Tivoli System Automation


Debe configurar un clúster de IBM Spectrum Protect para utilizar Tivoli System Automation.

Procedimiento

1. Instale y configure los componentes de IBM Spectrum Protect en los nodos primario y secundario.
2. Instale Tivoli System Automation en los nodos primario y secundario.
3. Configure los recursos de almacenamiento.
4. Dependiendo de la versión de IBM Spectrum Protect instalada en el servidor, es posible que tenga que actualizar el servidor de IBM Spectrum Protect para el clúster de Tivoli System Automation.
5. Opcional: Puede establecer la variable `FILE_EXIT` en el script de clúster `tsmserverctrl` para direccionar los datos de sucesos de Tivoli System Automation al archivo `FILEEXIT` del servidor de IBM Spectrum Protect.

Por ejemplo, edite el script de clúster de tsmserverctrl en el directorio <server_install_directory>/tsam/controls y añada la siguiente línea:

```
FILE_EXIT="fileexittmp"
```

 Sistemas operativos Linux

Requisitos previos para configurar un entorno en clúster de Linux con Tivoli System Automation


Antes de instalar y configurar IBM Spectrum Protect en un entorno en clúster con Tivoli System Automation, debe comprobar los requisitos previos.

Compruebe que se cumplen los siguientes requisitos previos.

- Planifique la instalación del servidor de IBM Spectrum Protect.
- Después de instalar IBM Spectrum Protect, verifique los siguientes elementos:
 - Asegúrese de que la base de datos de DB2 está instalada en el mismo nodo que el servidor.
 - Compruebe que el servidor puede controlar la recuperación de la base de datos de control.
 - Compruebe que están disponibles los volúmenes de almacenamiento compartido. IBM Spectrum Protect requiere dispositivos de almacenamiento compartido de alta disponibilidad para proteger la integridad de datos.
 - Verifique que cada nodo del clúster puede contener varias instancias del servidor.
- Prepare la instalación de Tivoli System Automation. Para obtener instrucciones, vaya a la documentación de producto de Tivoli System Automation. En la *Guía de instalación y configuración*, busque *Preparación para la instalación*.
- Después de instalar Tivoli System Automation, compruebe que Tivoli System Automation puede procesar la migración tras error como migración tras error de la IP y la migración tras error de datos para la base de datos, la instancia de datos, los registros activos y de archivado, y las agrupaciones de almacenamiento.




Tareas relacionadas:

Planificación para instalar el servidor de IBM Spectrum Protect

 Sistemas operativos Linux

Instalación y configuración de componentes de IBM Spectrum Protect en los nodos primario y secundario

Debe instalar los componentes de base de datos y servidor de IBM Spectrum Protect en los nodos primario y secundario del clúster. A continuación, configure primero el nodo primario seguido del nodo secundario.

-  Sistemas operativos Linux Instalación de los componentes de servidor de IBM Spectrum Protect
Después de comprobar y verificar los requisitos previos, debe instalar los componentes requerido en los nodos primario y secundario del sistema.
-  Sistemas operativos Linux Configuración del nodo primario
Para establecer la topología de dos nodos, configure los componentes de IBM Spectrum Protect en ambos nodos. En primer lugar, debe configurar la instancia de IBM Spectrum Protect en el nodo primario.
-  Sistemas operativos Linux Configuración del nodo secundario
Después de configurar el nodo primario, debe configurar el nodo secundario para que Tivoli System Automation pueda mover los componentes de servidor de IBM Spectrum Protect al nodo secundario si el servidor falla en el nodo primario.

 Sistemas operativos Linux

Instalación de los componentes de servidor de IBM Spectrum Protect


Después de comprobar y verificar los requisitos previos, debe instalar los componentes requerido en los nodos primario y secundario del sistema.

Procedimiento

Revise los temas en la información de configuración de un servidor de IBM Spectrum Protect.

Tareas relacionadas:

Instalación de los componentes del servidor IBM Spectrum Protect

 Sistemas operativos Linux

Configuración del nodo primario

Para establecer la topología de dos nodos, configure los componentes de IBM Spectrum Protect en ambos nodos. En primer lugar, debe configurar la instancia de IBM Spectrum Protect en el nodo primario.

Antes de empezar

- Instale los componentes del servidor de IBM Spectrum Protect.
- Verifique que el propietario de instancia de IBM Spectrum Protect tiene el mismo ID de grupo y usuario para todos los nodos del dominio de clúster.
- Verifique que el propietario de instancia de IBM Spectrum Protect tiene la misma contraseña para todos los nodos del clúster.

Procedimiento

1. Para obtener instrucciones detalladas sobre cómo crear los directorios y el ID de usuario para la instancia de servidor, consulte Linux: Creación del ID de usuario y los directorios para la instancia de servidor.
2. Verifique que el servidor de IBM Spectrum Protect, la instancia de DB2 y los directorios de registro de archivado y activos se comparten.
3. Defina los puntos de montaje añadiendo entradas al archivo `/etc/fstab`.

Cuando añada puntos de montaje en los nodos de clúster, utilice la opción `noauto` para evitar que los puntos de montaje se monten automáticamente en más de un nodo del clúster.

4. Establezca los siguientes permisos en cada uno de los puntos de montaje:
 - 755. Por ejemplo, el mandato siguiente establece el permiso 755 en el punto de montaje `/tsminst1`.

```
chmod -R 755 /tsminst1
```

- El propietario de instancia de servidor de IBM Spectrum Protect. Por ejemplo, el mandato siguiente establece los permisos para el propietario de instancia.

```
chown -R tsminst1 /tsminst1
```

- Grupo de servidores de IBM Spectrum Protect al que pertenece el propietario de instancia. Por ejemplo, el mandato siguiente establece los permisos para el grupo del propietario de instancia.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Para obtener instrucciones detalladas sobre la configuración del servidor de IBM Spectrum Protect utilizando el asistente de configuración, consulte Linux: Configuración de IBM Spectrum Protect mediante el asistente de configuración. Compruebe que todos los directorios compartidos están montados en el nodo primario.
6. Inicie instancia de servidor de IBM Spectrum Protect en el nodo primario utilizando el programa de utilidad DSMSEVR. Por ejemplo, el mandato siguiente inicia el servidor para una operación normal.

```
/opt/tivoli/tsm/server/bin/dsmsevr
```

7. Verifique que los componentes de IBM Spectrum Protect se han iniciado sin errores.
8. Cierre el servidor IBM Spectrum Protect.
9. Como usuario `root`, desmonte las unidades compartidas.

 Sistemas operativos Linux

Configuración del nodo secundario

Después de configurar el nodo primario, debe configurar el nodo secundario para que Tivoli System Automation pueda mover los componentes de servidor de IBM Spectrum Protect al nodo secundario si el servidor falla en el nodo primario.

Procedimiento

1. Para crear manualmente los directorios y el ID de usuario para la instancia de servidor, siga las instrucciones de Creación del ID de usuario y los directorios para la instancia de servidor.
2. Verifique que el servidor de IBM Spectrum Protect, la instancia de DB2 y los directorios de registro de archivado y activos se comparten.
3. Defina los puntos de montaje añadiendo entradas al archivo `/etc/fstab`.

Cuando añada puntos de montaje en los nodos de clúster, utilice la opción noauto. Esta opción evita que los puntos de montaje se monten automáticamente en más de un nodo del clúster.

Compruebe que todos los directorios compartidos están montados en el nodo secundario.

4. Establezca los siguientes permisos en cada uno de los puntos de montaje:

- 755. Por ejemplo, el mandato siguiente establece el permiso 755 en el punto de montaje /tsminst1.

```
chmod -R 755 /tsminst1
```

- El propietario de instancia de servidor de IBM Spectrum Protect. Por ejemplo, el mandato siguiente establece los permisos para el propietario de instancia.

```
chown -R tsminst1 /tsminst1
```

- Grupo de servidores de IBM Spectrum Protect al que pertenece el propietario de instancia. Por ejemplo, el mandato siguiente establece los permisos para el grupo del propietario de instancia.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Cree una instancia de servidor de IBM Spectrum Protect emitiendo el mandato db2icrt. Para obtener instrucciones, consulte Creación de la instancia de servidor.

Recuerde: No es necesario que cree un archivo de opciones de servidor porque el nodo secundario utiliza el archivo dsmserv.opt del nodo primario.

Compruebe que todos los directorios compartidos están montados en el nodo secundario.

6. Catalogue la base de datos emitiendo el mandato catalog db. Por ejemplo, el mandato siguiente cataloga la base de datos tsmdb1.

```
db2 catalog db tsmdb1
```

7. Prepare la base de datos para la copia de seguridad. Para obtener instrucciones, consulte Preparación del gestor de bases de datos para la copia de seguridad de base de datos.

8. Inicie el servidor de IBM Spectrum Protect utilizando el programa de utilidad DSMSERV. Por ejemplo, el mandato siguiente inicia el servidor para una operación normal.

```
/opt/tivoli/tsm/server/bin/dsmserv
```








9. Verifique que los componentes de IBM Spectrum Protect se han iniciado sin errores.

10. En los nodos secundarios, cierre el servidor de IBM Spectrum Protect y desmonte los directorios compartidos.

 Sistemas operativos Linux

Instalación de Tivoli System Automation en nodos primario y secundario

Después de instalar y configurar IBM Spectrum Protect en los nodos primario y secundario del clúster, debe instalar y configurar Tivoli System Automation en esos nodos. A continuación, debe activar esos nodos para el dominio, configurar los recursos y activar la política base. Finalmente, debe añadir los puntos de montaje para los directorios de IBM Spectrum Protect.

-  Sistemas operativos Linux Creación de una etiqueta para los puntos de montaje
Cree una etiqueta para cada punto de montaje en los nodos primario y secundario del clúster.
-  Sistemas operativos Linux Instalación y configuración de Tivoli System Automation
Debe instalar IBM Tivoli System Automation for Multiplatforms en los nodos primario y secundario del sistema.
-  Sistemas operativos Linux Preparación para activar los nodos de clúster para el dominio
Después de instalar Tivoli System Automation en los nodos primario y secundarios del clúster, debe preparar estos nodos para poder activar el clúster e iniciar el dominio de clúster.
-  Sistemas operativos Linux Configuración de recursos del grupo de volúmenes
Si ha creado grupos de volúmenes para el clúster, debe configurar estos recursos. Tivoli System Automation encuentra y define automáticamente los recursos del volumen de disco compartido.
-  Sistemas operativos Linux Configuración de recursos que no están en un grupo de volúmenes
Si ha creado los recursos de *almacenamiento de disco compartido* utilizando los tipos de recurso ext2, ext3 o reiserfs en uno de los nodos del clúster, debe configurar estos recursos.
-  Sistemas operativos Linux Activación de la política base
Después de configurar los recursos, debe activar la política en los nodos primario y secundario para crear los recursos restantes y el grupo de recursos.
-  Sistemas operativos Linux Adición de puntos de montaje a directorios de IBM Spectrum Protect
Antes de poder iniciar el clúster, debe añadir los puntos de montaje que ha creado para los componentes de IBM Spectrum Protect.

 Sistemas operativos Linux

Creación de una etiqueta para los puntos de montaje

Cree una etiqueta para cada punto de montaje en los nodos primario y secundario del clúster.


Procedimiento

1. Cree una etiqueta para cada uno de los volúmenes que ha creado anteriormente para los puntos de montaje del directorio compartido emitiendo el mandato `e2label`. Por ejemplo, el mandato siguiente crea la etiqueta `/tsminst1` que tiene una partición `/dev/tsmvg1/tsminst1LV`.

```
e2label /dev/tsmvg1/tsminst1LV /tsminst1
```

2. Para cada nodo del clúster, sustituya las entradas para los puntos de montaje que ha creado anteriormente en el archivo `/etc/fstab`. Por ejemplo, para la etiqueta de ejemplo anterior, emita el mandato siguiente:

```
LABEL=/tsminst1 /tsminst1 ext3 defaults 0 0
```

 Sistemas operativos Linux


Instalación y configuración de Tivoli System Automation


Debe instalar IBM® Tivoli System Automation for Multiplatforms en los nodos primario y secundario del sistema.

Procedimiento

1. Para instalar y configurar Tivoli System Automation, existe información detallada en la Tivoli System Automation Guía de instalación y configuración.
2. Descargue el archivo `TSM-25072011-1015.zip` de Integrated Service Management Library. Extraiga el archivo comprimido en cada uno de los nodos de clúster.
3. Después de extraer el archivo comprimido, verifique que el nuevo directorio de Tivoli System Automation creado durante la instalación incluye el directorio `/TSM/HA` y subdirectorios.

Información relacionada:

 Información sobre el producto IBM Tivoli System Automation for Multiplatforms versión 3.2.2

 Sistemas operativos Linux

Preparación para activar los nodos de clúster para el dominio

Después de instalar Tivoli System Automation en los nodos primario y secundarios del clúster, debe preparar estos nodos para poder activar el clúster e iniciar el dominio de clúster.

Procedimiento

1. Prepare cada uno de los nodos para el dominio emitiendo el mandato `preprnode`. Emita este mandato para todos los nodos de clúster del dominio. Por ejemplo, el mandato siguiente prepara los nodos `HOST1.ibm.com` y `HOST2.ibm.com`.

```
preprnode HOST1.ibm.com HOST2.ibm.com
```

2. Cree un dominio para cada nodo emitiendo el mandato `mkrpdomain`. Por ejemplo, el mandato siguiente crea `tsm_domain` para los nodos `HOST1.ibm.com` y `HOST2.ibm.com`.

```
mkrpdomain tsm_domain HOST1.ibm.com HOST2.ibm.com
```

3. Inicie el dominio para cada nodo emitiendo el mandato `starttrpdomain`. Por ejemplo, el mandato siguiente inicia `tsm_domain`.

```
starttrpdomain tsm_domain
```

 Sistemas operativos Linux

Configuración de recursos del grupo de volúmenes

Si ha creado grupos de volúmenes para el clúster, debe configurar estos recursos. Tivoli System Automation encuentra y define automáticamente los recursos del volumen de disco compartido.

Procedimiento

Para configurar los recursos de grupo de volúmenes para los directorios de IBM Spectrum Protect compartidos y montar puntos que ha creado anteriormente, complete los pasos siguientes en el nodo primario.

1. Importe los grupos de volúmenes. Por ejemplo, utilice el mandato `vgimport X` para importar los grupos de volúmenes `X`.
2. Active los grupos de volúmenes. Por ejemplo, utilice el mandato `vgchange -ay X` para activar los grupos de volúmenes `X`.
3. Monte el sistema de archivos emitiendo el mandato `mount`. El ejemplo siguiente monta el sistema de archivos `X`.

```
mount X
```

4. Reinicie el dominio emitiendo los mandatos `stoprpdomain` y `startrpdomain`. Por ejemplo, los mandatos siguientes reinician `tsm_domain`.

```
stoprpdomain tsm_domain
startrpdomain tsm_domain
```

5. Desmonte el sistema de archivos emitiendo el mandato `umount`. Por ejemplo, utilice el mandato `umount X` para desmontar el sistema de archivos `X`.
6. Desactive los grupos de volúmenes. Por ejemplo, utilice el mandato `vgchange -an X` para desactivar los grupos de volúmenes `X`.
7. Verifique que todos los recursos de almacenamiento IBM®.AgfileSystem se recolectan mediante Tivoli System Automation emitiendo el mandato siguiente:

```
lsrsrc -s "Name=='Resource_Name' && ResourceType=1" IBM.AgFileSystem
```



Configuración de recursos que no están en un grupo de volúmenes

Si ha creado los recursos de *almacenamiento de disco compartido* utilizando los tipos de recurso `ext2`, `ext3` o `reiserfs` en uno de los nodos del clúster, debe configurar estos recursos.

Procedimiento

Complete los siguientes pasos en el servidor primario.

1. Monte el sistema de archivos emitiendo el mandato `mount`. Por ejemplo, el mandato siguiente monta el sistema de archivos `X`.

```
mount X
```

2. Reinicie el dominio emitiendo los mandatos `stoprpdomain` y `startrpdomain`. Por ejemplo, el mandato siguiente reinicia `tsm_domain`.

```
stoprpdomain tsm_domain
startrpdomain tsm_domain
```

3. Desmonte el sistema de archivos emitiendo el mandato `umount`. Por ejemplo, el mandato siguiente desmonta el sistema de archivos `X`.

```
umount X
```

4. Verifique que todos los recursos de almacenamiento IBM®.AgfileSystem se recolectan mediante Tivoli System Automation emitiendo el mandato siguiente:

```
lsrsrc -s "Name=='Resource_Name' && ResourceType=1" IBM.AgFileSystem
```


Por ejemplo, para verificar el recurso `tsmalog`, ejecute el siguiente mandato:

```
lsrsrc -s "Name=='tsmalog' && ResourceType=1" IBM.AgFileSystem
Resource Persistent Attributes for IBM.AgFileSystem resource 1:
ResourceHandle= "0x2038 0xffff 0x6ad47197 0x256fc23d 0x9338a9950x263fa510"
Name           = "tsmalog"
ResourceType   = 1 <-----
MountPoint     = ""
DeviceName     = ""
Vfs            = "ext3"
AggregateResource = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000 0x00000000"
ContainerResource = "0x2036 0xffff 0x6ad47197 0x256fc23d 0x9338a995 0x25ffaa28"
GhostDevice    = 0
ResourceId     = "360050768019c021d30000000000005da"
ProtectionMode = 1
```

```

UserControl          = 0
SysMountPoint       = "/tsmalog"
Label                = "/tsmalog"
FSID                 = "5792f887-8547-4c33-a519-9d0c50ab6882"
PreOnlineMethod     = 0
ContainerResourceId = "360050768019c021d30000000000005da"
AutoMonitor         = 1
Options              = "defaults,noauto"
PreOfflineMethod    = 0
ActivePeerDomain    = "TSM_Domain"
NodeNameList        =
{"tsmlnode01.storage.tucson.ibm.com","tsmlnode02.storage.tucson.ibm.com"}

```

 Sistemas operativos Linux

Activación de la política base

Después de configurar los recursos, debe activar la política en los nodos primario y secundario para crear los recursos restantes y el grupo de recursos.

Acerca de esta tarea

Para activar la política base, debe crear el recurso IP de servicio y los recursos de aplicación de IBM Spectrum Protect para los recursos de aplicación de la instancia de servidor de IBM Spectrum Protect. A continuación, debe crear el grupo de recursos y las políticas para gestionar el clúster.

Procedimiento

Complete los pasos siguientes primero en el nodo primario y, después, en el nodo secundario.

1. Vaya al directorio donde extrajo el contenido del archivo TSM-25072011-1015.zip.
2. Establezca los permisos de archivos en los scripts del directorio bin emitiendo el mandato `chmod`. Por ejemplo, el mandato siguiente establece los permisos de archivo para todos los scripts del directorio bin. XXX es el nombre de la carpeta extraída.

```
chmod 755 /XXX/TSM/HA/bin/*
```

3. Vaya al directorio bin emitiendo el mandato `cd`.
4. Actualice las variables siguientes en el script `base_cluster_variables.sh`:
 - o `NODE1` especifica el nombre de host para el nodo 1 (nodo primario) del clúster.
 - o `NODE2` especifica el nombre de host para el nodo 2 (nodo secundario) del clúster.
 - o `IP_GATEWAY` especifica la pasarela de la IP de servicio.
 - o `SUBNET_MASK` especifica la máscara de subred de la IP de servicio.
 - o `NET_INT` especifica el nombre de la interfaz de red de un nodo específico del clúster. El nombre debe ser el mismo para todos los nodos del clúster.
5. Ejecute el script de configuración de `configureHA.sh` emitiendo el mandato `./configureHA.sh` en todos los nodos del clúster. Si el script `configureHA.sh` falla con el error `-bash: ./configureHA.sh: /bin/bash^M: bad interpreter: No such file or directory`, emita el mandato `dos2unix` en todos los scripts del directorio bin. Por ejemplo, para cada script, ejecute el mandato siguiente:

```
dos2unix -o <filename>
```

6. Verifique que la configuración es un éxito verificando que los scripts de configuración se ejecutan correctamente.
7. Atención: Complete este paso únicamente en el nodo primario. Ejecute el script de configuración emitiendo el mandato `./setup.sh`. Por ejemplo, el mandato siguiente ejecuta el script de configuración en la instancia de servidor de `inst1` IBM Spectrum Protect para el usuario de instancia `dbinst1` del directorio de instancia de servidor `/tsminst1` IBM Spectrum Protect con `9.11.142.129` como IP de servicio.

```
./setup.sh inst1 dbinst1 /tsminst1 9.11.142.129
```

8. Compruebe que está utilizando la IP correcta ejecutando el siguiente mandato:

```
lssam -V
```

9. Repita el paso 5 para todas las instancias de IBM Spectrum Protect que tiene en el entorno de servidor de IBM Spectrum Protect.
10. Complete todos los pasos anteriores en el nodo secundario.

 Sistemas operativos Linux

Adición de puntos de montaje a directorios de IBM Spectrum Protect

Antes de poder iniciar el clúster, debe añadir los puntos de montaje que ha creado para los componentes de IBM Spectrum Protect.

Procedimiento

Para añadir puntos de montaje de disco compartido al grupo de recursos de clúster y poner al clúster en línea, complete los pasos siguientes:

1. Identifique los puntos de montaje para los siguientes directorios:

- o Instancia
- o Base de datos
- o Registro activo
- o Registro de archivado
- o Agrupación de almacenamiento

2. Añada recursos a cada punto de montaje:

- a. Compruebe si el grupo de recursos `tsm-$INST_NAME-rg` está en línea emitiendo el mandato `lssam`.
- b. Si el grupo de recursos `tsm-$INST_NAME-rg` está en línea, póngalo fuera de línea emitiendo el siguiente mandato:

```
chrg -o offline tsm-$INST_NAME-rg
```


- c. Vaya al directorio donde extrajo el contenido del archivo `TSM-25072011-1015.zip`.
- d. Vaya al directorio `bin` emitiendo el mandato `cd`.
- e. Para añadir recursos de disco compartido a cada punto de montaje, ejecute el script `./update_setup.sh`. Por ejemplo, el mandato siguiente añade el punto de montaje `/tsminst1` a la instancia de servidor `inst1` IBM Spectrum Protect.

```
./update_setup.sh inst1 /tsminst1
```

3. Ponga el grupo de recursos `tsm-$INST_NAME-rg` en línea emitiendo el mandato siguiente:




```
chrg -o online tsm-$INST_NAME-rg
```

4. Conéctese al servidor mediante un IP de pasarela de servicio para comprobar que la configuración es correcta.

 Sistemas operativos Linux

Configuración de recursos de almacenamiento

Utilice la interfaz de usuario de Tivoli System Automation o de la línea de mandatos para añadir o suprimir los recursos de almacenamiento y para suprimir los puntos de montaje que ya no son necesarios. Si añade una agrupación de almacenamiento al clúster, debe añadirla al grupo de recursos. Si elimina una agrupación de almacenamiento del clúster, también debe suprimirla del grupo de recursos.

-  Sistemas operativos Linux Adición de una agrupación de almacenamiento a un grupo de recursos
Si la configuración de IBM Spectrum Protect almacena datos en discos, debe añadir el punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos.
-  Sistemas operativos Linux Supresión de una agrupación de almacenamiento de un grupo de recursos
Puede suprimir una agrupación de almacenamiento que ya no se necesita. Si se elimina una agrupación de almacenamiento de la instancia de servidor de IBM Spectrum Protect, debe suprimirse del grupo de recursos.
-  Sistemas operativos Linux Supresión de un punto de montaje de un grupo de recursos
Puede que desee eliminar un punto de montaje que ya no se necesita.

 Sistemas operativos Linux

Adición de una agrupación de almacenamiento a un grupo de recursos

Si la configuración de IBM Spectrum Protect almacena datos en discos, debe añadir el punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos.

Procedimiento

Para añadir un punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos, complete los pasos siguientes:

1. Bloquee el grupo de recursos emitiendo el mandato `rgreq -o lock`. Por ejemplo, el mandato siguiente bloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o lock Sample_Resourcegroup_X
```

2. Vaya al directorio `bin` emitiendo el mandato `cd`.
3. Para añadir un recurso de agrupación de almacenamiento para un grupo de recursos, ejecute el script `update_setup.sh` emitiendo el mandato `./update_setup.sh`. Por ejemplo, el mandato siguiente añade el punto de montaje de la agrupación de almacenamiento `/inst1stg1` a la instancia de servidor `inst1` de IBM Spectrum Protect.

```
./update_setup.sh inst1 /inst1stg1
```

4. Desbloquee el grupo de recursos emitiendo el mandato `rgreq -o unlock`. Por ejemplo, el mandato siguiente desbloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o unlock Sample_Resourcegroup_X
```



Sistemas operativos Linux

Supresión de una agrupación de almacenamiento de un grupo de recursos

Puede suprimir una agrupación de almacenamiento que ya no se necesita. Si se elimina una agrupación de almacenamiento de la instancia de servidor de IBM Spectrum Protect, debe suprimirse del grupo de recursos.

Procedimiento

Para suprimir una agrupación de almacenamiento, complete los pasos siguientes:

1. Bloquee el grupo de recursos emitiendo el mandato `rgreq -o lock`. Por ejemplo, el mandato siguiente bloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o lock Sample_Resourcegroup_X
```

2. Vaya al directorio `bin` emitiendo el mandato `cd`.
3. Para suprimir un recurso de agrupación de almacenamiento de un grupo de recursos, ejecute el script `delete_mount.sh` emitiendo el mandato `./delete_mount.sh`. Por ejemplo, el mandato siguiente suprime el punto de montaje `/inst1stg1` de la instancia de servidor `inst1` IBM Spectrum Protect.

```
./delete_mount.sh /inst1stg1 inst1
```

4. Desbloquee el grupo de recursos emitiendo el mandato `rgreq -o unlock`. Por ejemplo, el mandato siguiente desbloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o unlock Sample_Resourcegroup_X
```



Sistemas operativos Linux

Supresión de un punto de montaje de un grupo de recursos

Puede que desee eliminar un punto de montaje que ya no se necesita.

Procedimiento

Para suprimir un punto de montaje, complete los pasos siguientes:

1. Compruebe si el grupo de recursos `tsm- $\$$ INST_NAME-rg` está en línea emitiendo el mandato `lssam`.
2. Si el grupo de recursos `tsm- $\$$ INST_NAME-rg` está en línea, póngalo fuera de línea emitiendo el siguiente mandato:

```
chrg -o offline tsm- $\$$ INST_NAME-rg
```

3. Vaya al directorio `bin` emitiendo el mandato `cd`.
4. Para suprimir un punto de montaje, ejecute el script `delete_mount.sh`. Por ejemplo, el mandato siguiente suprime el punto de montaje `/tsminst1` del grupo de recursos de la instancia de servidor `inst1` IBM Spectrum Protect.

```
./delete_mount.sh /tsminst1 inst1
```

5. Ponga el grupo de recursos `tsm- $\$$ INST_NAME-rg` en línea emitiendo el mandato siguiente:

```
chrg -o online tsm- $\$$ INST_NAME-rg
```

Actualización de un servidor configurado con Tivoli System Automation

Puede actualizar un servidor configurado con Tivoli System Automation desde la Versión 6.3 o la Versión 7.1.

Procedimiento

Para actualizar el servidor en todos los nodos del clúster, inicie la sesión en el servidor y siga los pasos siguientes. Estos pasos inician la actualización en el nodo primario y, después, la última parte de este procedimiento actualiza el nodo secundario.

1. Detenga los recursos del servidor emitiendo el mandato `chrg -o Offline`. Por ejemplo, el mandato siguiente detiene los recursos del grupo de recursos `tsm-tsminst1-rg`:

```
chrg -o Offline tsm-tsminst1-rg
```

2. Detenga el dominio de Tivoli System Automation emitiendo el mandato `stoprpdomain`. Por ejemplo, el mandato siguiente detiene `tsm_domain`:

```
stoprpdomain tsm_domain
```

3. Monte los puntos de montaje del servidor en el nodo primario.
4. Para actualizar el servidor en el nodo primario, consulte Actualización de IBM Spectrum Protect.
5. Después de que la actualización haya finalizado, complete los pasos posteriores a la actualización para verificar que la actualización se ha realizado correctamente en el nodo primario.
6. Detenga el servidor y desmonte los puntos de montaje del servidor en el nodo primario.
7. Monte los puntos de montaje del servidor en el nodo secundario.
8. Si está actualizando un servidor de la V6 a la V7, realice los pasos siguientes:
 - a. Desinstale el servidor.

Para obtener las instrucciones, consulte Desinstalación del servidor V6.3.

- b. Instale el servidor en el nodo secundario. Siga las instrucciones de Linux: Instalación de los componentes de servidor.
9. Para actualizar el servidor en el nodo secundario, consulte Actualización del servidor.
 10. Después de que la actualización haya finalizado, complete los pasos posteriores a la actualización para verificar que la actualización se ha realizado correctamente en el nodo secundario.
 11. Desmonte los puntos de montaje del servidor en el nodo secundario.
 12. Inicie el dominio de Tivoli System Automation emitiendo el mandato `startrpdomain`. Por ejemplo, el mandato siguiente inicia `tsa_domain`:

```
startrpdomain tsa_domain
```

13. Inicie los recursos del servidor emitiendo el mandato `chrg -o Online`. Por ejemplo, el mandato siguiente inicia los recursos del grupo de recursos `tsm-tsminst1-rg`:


```
chrg -o Online tsm-tsminst1-rg
```

Configuración de un entorno en clúster de Windows





Puede configurar un servidor de IBM Spectrum Protect para Windows en un entorno de clúster de migración tras error de Microsoft. Los entornos de clúster de Windows están formados por componentes como, por ejemplo, servidores IBM Spectrum Protect, hardware y software. Si estos componentes están conectados al mismo sistema de disco el tiempo de inactividad se minimiza.


El software de Microsoft permite configurar, supervisar y controlar componentes de hardware y aplicaciones que están en un clúster de Windows. El administrador utiliza la interfaz del administrador de clústeres de Microsoft y IBM Spectrum Protect para designar organizaciones de clústeres y definir el patrón de recuperación de errores.

IBM Spectrum Protect soporta la migración tras error de cintas para un entorno de clúster utilizando una conexión de fibra o SCSI. Aunque los clústeres de migración tras error de Microsoft no dan soporte a la migración tras error de los dispositivos de cinta, la configuración de la migración tras error puede supervisarse con la interfaz de Microsoft Cluster Administrator después de que se configure en IBM Spectrum Protect.

-  Sistemas operativos Windows Visión general del entorno de Microsoft Failover Cluster
Con un Microsoft Failover Cluster Manager, puede colocar recursos de un clúster de servidores de IBM Spectrum Protect en un

grupo de clústeres. El grupo de clústeres de IBM Spectrum Protect tiene un nombre de red, una dirección IP, uno o varios discos físicos, un servidor DB2 y un servicio de servidor de IBM Spectrum Protect.

-  Sistemas operativos Windows Recuperación de errores de cinta para los nodos de un clúster
Los grupos de un clúster pueden transferirse a otros nodos si el nodo que aloja los grupos falla.
-  Sistemas operativos Windows Planificación de un entorno en clúster
La configuración en un entorno en clúster requiere una planificación para garantizar el rendimiento óptimo del sistema. La decisión de configurar el sistema para incluir clústeres depende de las necesidades de su negocio.
-  Sistemas operativos Windows Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster
Debe asegurarse de que el clúster esté instalado y configurado correctamente antes de instalar IBM Spectrum Protect.
-  Sistemas operativos Windows Mantenimiento del entorno en clúster
Después de configurar el clúster o los clústeres iniciales, las necesidades de mantenimiento son mínimas.

 Sistemas operativos Windows

Visión general del entorno de Microsoft Failover Cluster

Con un Microsoft Failover Cluster Manager, puede colocar recursos de un clúster de servidores de IBM Spectrum Protect en un grupo de clústeres. El grupo de clústeres de IBM Spectrum Protect tiene un nombre de red, una dirección IP, uno o varios discos físicos, un servidor DB2 y un servicio de servidor de IBM Spectrum Protect.

El nombre de red de la instancia de IBM Spectrum Protect es independiente del nombre del nodo físico en el que se ejecuta el grupo de clústeres de IBM Spectrum Protect y se migra de nodo a nodo. Los clientes se conectan a un servidor de IBM Spectrum Protect utilizando el nombre de red de la instancia, en lugar del nombre de nodo de Windows. El nombre de red de instancia se correlaciona con un nodo primario o de seguridad. La correlación depende del nodo que es propietario del grupo de clústeres. Un cliente que utilice WINS (Windows Internet Name Service) o servicios de directorio para localizar servidores puede realizar automáticamente un seguimiento del servidor en clúster de IBM Spectrum Protect cuando se mueve entre los nodos. Puede realizar automáticamente un seguimiento del servidor en clúster sin modificar o volver a configurar el cliente.

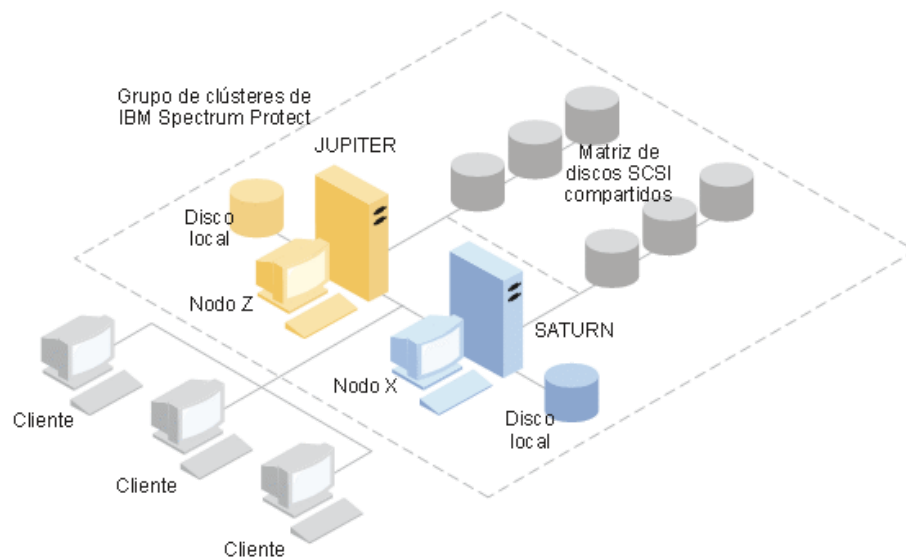
Cada grupo de clústeres de IBM Spectrum Protect tiene su propio disco como parte de un grupo de recursos de clúster. Los grupos de clústeres de IBM Spectrum Protect no pueden compartir datos entre los grupos de clústeres. Cada servidor de IBM Spectrum Protect que se ha configurado en un grupo de clústeres tiene sus propias bases de datos, registros activos, registros de recuperación y conjunto de volúmenes de agrupación de almacenamiento en un disco independiente. Este disco es propiedad del grupo de clústeres donde está configurado el servidor.

Recuerde: Microsoft Failover Cluster Manager sólo da soporte a una dirección IP como recurso. Esto significa que los servidores de IBM Spectrum Protect que se ejecuten en un clúster deben limitar su método de comunicación soportado a sólo TCP/IP. Un cliente que no utilice TCP/IP como método de comunicación no podrá acceder al grupo de clústeres de IBM Spectrum Protect si realiza la migración tras error en el otro nodo de clúster.

El siguiente ejemplo muestra cómo funciona un Microsoft Failover Cluster Manager para un servidor de clúster de IBM Spectrum Protect.

Supongamos que un servidor de IBM Spectrum Protect en clúster denominado JUPITER se ejecuta en el nodo Z y un servidor de IBM Spectrum Protect en clúster denominado SATURN se ejecuta en el nodo X. Los clientes se conectan al servidor de IBM Spectrum Protect JUPITER y al servidor de IBM Spectrum Protect SATURN sin saber qué nodo aloja actualmente su servidor.

Figura 1. Agrupación en clúster con JUPITER como nodo Z y SATURN como nodo X



Cuando falla uno de los recursos de software o de hardware, se produce una recuperación de errores. Los recursos como las aplicaciones, discos y una dirección IP se mueven del nodo con errores al otro nodo. El nodo restante:

- Toma el control del grupo de clústeres de IBM Spectrum Protect
- Pone en línea los recursos de disco, los recursos de red y el recurso de DB2
- Reinicia el servicio de IBM Spectrum Protect

- Proporciona acceso a los administradores y los clientes


Si el nodo X falla, el nodo Z asume el rol de ejecutar SATURN. Para un cliente, es exactamente igual que si se desactiva el nodo X y se vuelve a activar inmediatamente. Los clientes experimentan la pérdida de todas las conexiones con SATURN y todas las transacciones activas se retrotraen al cliente. Los clientes deben volver a conectarse con SATURN una vez perdida la conexión. La ubicación de SATURN no es aparente para el cliente.

 Sistemas operativos Windows

Recuperación de errores de cinta para los nodos de un clúster

Los grupos de un clúster pueden transferirse a otros nodos si el nodo que aloja los grupos falla.

Un nodo puede alojar unidades físicas o lógicas, denominadas recursos. Los administradores organizan estos recursos de clúster en unidades funcionales denominadas grupos y asignan estos grupos a nodos individuales. Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.

-  Sistemas operativos Windows Recuperación de errores de cinta de fibra
IBM Spectrum Protect puede gestionar la recuperación de errores de los dispositivos de cinta y biblioteca con conexión directa de canal de fibra en un sistema Microsoft Windows en un entorno en clúster sin necesidad de hardware adicional.

 Sistemas operativos Windows

Planificación de un entorno en clúster

La configuración en un entorno en clúster requiere una planificación para garantizar el rendimiento óptimo del sistema. La decisión de configurar el sistema para incluir clústeres depende de las necesidades de su negocio.




Planifique una configuración de clústeres que se adapte a su entorno. Además de comprobar que tiene el tipo correcto de hardware y el software aplicable, debe configurar un patrón de migración tras error.

Cuando un nodo falla o necesita ponerse fuera de línea, ¿qué nodo o nodos del clúster continúan con el proceso de las transacciones? En un clúster de dos nodos, se necesita poca planificación. En un clúster más complejo, debe tener en cuenta cómo se maneja mejor el proceso de las transacciones. Es preciso prever algún tipo de equilibrio de carga entre los nodos para mantener un rendimiento óptimo. También es preciso asegurarse de que sus clientes no puedan percibir ningún retraso ni un descenso en la productividad.

Microsoft Cluster Servers y Microsoft Failover Clusters requieren que cada instancia de servidor de IBM Spectrum Protect tenga un conjunto privado de recursos de disco. Aunque los nodos pueden compartir recursos de disco, sólo un nodo puede controlar activamente un disco cada vez.


Atención: Asegúrese de que se haya instalado el mismo nivel de Windows (Windows 2012, Windows 2012 R2 y Windows 2016) en todos los sistemas del clúster.

¿Qué configuración es mejor? Para determinar cuál es la mejor instalación, analice las diferencias de rendimiento y de coste. Supongamos que tiene un clúster de servidores dedicados de IBM Spectrum Protect cuyos nodos tienen una potencia comparable. Durante la migración tras error, el rendimiento de una configuración puede disminuir porque un nodo debe gestionar las dos instancias de clúster de IBM Spectrum Protect. Si cada nodo gestiona 100 clientes en una operación normal, durante una anomalía un nodo gestiona 200 clientes.

-  Sistemas operativos Windows Hoja de trabajo de configuración del clúster
Registre sus respuestas a las siguientes preguntas de planificación antes de realizar la configuración del clúster.
-  Sistemas operativos Windows Planificación de la configuración de hardware y software del clúster
La configuración de hardware y software del clúster se determina durante la fase de planificación y antes de la instalación.
-  Sistemas operativos Windows Configuración de IBM Spectrum Protect en Microsoft Failover Cluster
El procedimiento de configuración de clúster de IBM Spectrum Protect debe completarse en el conjunto de nodos que alojan un grupo de clústeres de IBM Spectrum Protect.

Información relacionada:

 Sistemas operativos soportados de IBM Spectrum Protect

 Sistemas operativos Windows

Hoja de trabajo de configuración del clúster

Registre sus respuestas a las siguientes preguntas de planificación antes de realizar la configuración del clúster.

1. ¿Qué tipo de solución de clúster se ajusta mejor a las necesidades de su negocio?
2. ¿Qué tipo de patrón de migración tras error necesita?


La utilización del soporte para la recuperación de errores de cinta también afectará a este patrón.

3. ¿Será necesario el soporte de migración tras error de cinta?

Tenga en cuenta cómo se utilizan los dispositivos de cinta en las instancias de clúster de IBM Spectrum Protect. La forma en la que las instancias de clúster utilizan los dispositivos de cinta puede limitar el número de nodos del patrón de migración tras error a dos.

4. ¿Cuáles son los recursos que se dedican a IBM Spectrum Protect?

Tipo de recurso	Nombre de recurso
Grupo de recursos de clúster	
Recursos de disco físico	
Dirección IP	
Máscara de subred	
Red	
Nombre de red (nombre del servidor)	
Nodos	
Recuperación de errores de cinta (opcional): nombre de dispositivo - ambos nodos	

 Sistemas operativos Windows

Planificación de la configuración de hardware y software del clúster

La configuración de hardware y software del clúster se determina durante la fase de planificación y antes de la instalación.

Procedimiento


Las siguientes directrices permiten determinar qué recursos son necesarios para que el clúster de IBM Spectrum Protect sea satisfactorio:

1. Decida qué configuración de clúster debe utilizar con los servidores que utilizan dispositivos de disco. Cada instancia de clúster de IBM Spectrum Protect necesita un conjunto aparte de recursos de disco en el subsistema de disco compartido. Es posible que tenga problemas si configura el subsistema de E/S como una matriz de gran tamaño. Por ejemplo, cuando configura un clúster de dos servidores y más adelante decide ampliar a un clúster de cuatro servidores.
2. Identifique los recursos de disco que se van a dedicar a IBM Spectrum Protect. No divida un disco compartido en varias particiones con cada partición asignada a una aplicación diferente y, por lo tanto, a un grupo de clúster diferente.

Por ejemplo, la aplicación A, una aplicación estable, puede verse obligada a una migración tras error debido a un problema de software con la aplicación B. Esta migración tras error se puede producir si ambas aplicaciones utilizan particiones que forman parte del mismo disco físico. Este problema provoca una recuperación de errores de los servicios de clúster en la aplicación B y su recurso de disco de correquisito. Como las particiones están en el mismo disco físico, también se fuerza la recuperación de errores de la aplicación A. Por lo tanto, al instalar y configurar una aplicación de IBM Spectrum Protect, dedique un disco compartido como recurso que se pueda recuperar si es necesario.

3. Asegúrese de tener la dirección IP y el nombre de red de cada una de las instancias del servidor de IBM Spectrum Protect que configure. Para un clúster que implique a dos instancias de clúster de IBM Spectrum Protect, se necesitan dos nombres de red.
4. Cree un grupo de recursos de clúster y traspase los recursos de disco a él. Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster. Inicialmente, el grupo debe contener solamente recursos de disco. O bien, puede optar por cambiar el nombre de un grupo de recursos existente que contenga sólo recursos de disco.
5. IBM Spectrum Protect se instala en un disco local en cada nodo del clúster. Determine el disco que debe utilizarse en cada nodo. Utilice la misma letra de unidad en cada sistema. Cuando el servidor de IBM Spectrum Protect está instalado en un entorno de clúster, la opción SANDISCOVERY debe establecerse en ON. De forma predeterminada, esta opción está establecida en OFF.
6. SI decide no utilizar el soporte de migración tras error de cintas de IBM Spectrum Protect, puede conectar dispositivos de cinta en cualquiera de las configuraciones siguientes:

Configuración	Ventajas e inconvenientes	El espacio de disco necesario	Cómo habilitar la migración	Qué hacer cuando se produce una migración tras error
Conectarlos al nodo en el que la instancia del servidor de IBM Spectrum Protect está activa actualmente.	Esta configuración permite operaciones de copia de seguridad y restauración de alto rendimiento. Sin embargo, no está completamente automatizada porque se necesita la intervención del operador para dar servicio a una recuperación de errores cuando se producen retardos de reparación.	Defina suficiente espacio de volumen para los datos basados en disco para mantener el promedio equivalente a más de dos días de datos.	Establezca una jerarquía de agrupaciones de almacenamiento para mover los datos eficazmente al dispositivo de cinta.	Desconecte manualmente el dispositivo de cinta y vuelva a conectarlo al nodo en el que se ha activado el servidor.
Conectarlos a un tercer sistema sin clúster en el que hay activa una instancia adicional del servidor de IBM Spectrum Protect.	Puede que esta configuración no sea viable en instalaciones con comunicaciones de ancho de banda bajo entre los servidores del clúster y el servidor de controlador de dispositivo de cinta.	Defina suficiente espacio de volumen para los datos basados en disco para mantener el promedio equivalente a más de dos días de datos.	Utilice los volúmenes virtuales para mover los datos de los volúmenes de disco locales al dispositivo de cinta.	No se requiere ninguna acción; el servidor activado continúa utilizando los volúmenes virtuales.


 Sistemas operativos Windows

Configuración de IBM Spectrum Protect en Microsoft Failover Cluster

El procedimiento de configuración de clúster de IBM Spectrum Protect debe completarse en el conjunto de nodos que alojan un grupo de clústeres de IBM Spectrum Protect.

Los pasos del procedimiento varían dependiendo del nodo donde realice la configuración actualmente. Cuando configura el nodo primario en el conjunto, se crea y se configura la instancia de servidor de IBM Spectrum Protect. Cuando configura los demás nodos del conjunto, cada nodo se actualiza utilizando un método específico. La forma en la que se actualiza el nodo le permite alojar la instancia de servidor de IBM Spectrum Protect creada en el nodo primario. Debe instalarse y configurarse un servidor de IBM Spectrum Protect en el primer nodo del conjunto antes de configurar los demás nodos del conjunto. El incumplimiento de este requisito hará que la configuración falle.

Asegúrese de configurar completamente un grupo de clústeres de IBM Spectrum Protect antes de continuar en el paso siguiente cuando configure varios grupos de clústeres de IBM Spectrum Protect. Como trabaja con direcciones IP y nombres de red diferentes para cada grupo de clústeres de IBM Spectrum Protect, disminuye la posibilidad de errores al configurar cada grupo de clústeres por separado.

 Sistemas operativos Windows

Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster

Debe asegurarse de que el clúster esté instalado y configurado correctamente antes de instalar IBM Spectrum Protect.


Procedimiento

Para configurar IBM Spectrum Protect en un Microsoft Failover Cluster, siga estos pasos:

1. Asegúrese de que el sistema operativo de Windows esté instalado en todos los sistemas que formen parte del clúster. Para obtener la información más actual sobre los sistemas operativos Windows soportados, consulte la nota técnica 1243309.
2. Inicie sesión con el ID de usuario de dominio. El usuario de dominio debe estar en el mismo dominio que el servidor de IBM Spectrum Protect.
3. Asegúrese de que el clúster de recuperación de errores esté instalado y configurado para todos los sistemas del clúster. Si tiene previsto instalar el servidor de IBM Spectrum Protect en el sistema operativo Windows Server 2012, instale antes el servidor de automatización de clúster de migración tras error y la interfaz de mandatos de clúster de migración tras error. Para instalar estos componentes, emita los siguientes mandatos desde Windows 2.0 PowerShell:


```
Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
```

4. Compruebe que todos los nodos y discos compartidos del clúster estén operativos.
 5. Asegúrese de que los dispositivos de cinta compartidos estén operativos si se está utilizando el soporte de recuperación de errores de cintas de IBM Spectrum Protect.
-  Sistemas operativos Windows Preparación de un grupo de Microsoft Failover Cluster para un servidor virtual básico
Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster.
 -  Sistemas operativos Windows Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster
Instale el servidor de IBM Spectrum Protect en cada nodo del clúster que aloje un servidor en clúster de IBM Spectrum Protect.
 -  Sistemas operativos Windows Inicialización del servidor de IBM Spectrum Protect para un Microsoft Failover Cluster en el nodo primario
Después de instalar IBM Spectrum Protect en los nodos del clúster, debe inicializar el servidor en el nodo primario.
 -  Sistemas operativos Windows Verificación de la configuración de IBM Spectrum Protect en un Microsoft Failover Cluster
Cuando termine de configurar IBM Spectrum Protect en un Microsoft Failover Cluster, puede revisar la ventana de resumen de Failover Cluster Manager. Verifique que la agrupación en clúster se haya completado correctamente y que el servidor de IBM Spectrum Protect se haya iniciado.
 -  Sistemas operativos Windows Prueba de recuperación de errores para el clúster
Después de completar la configuración de clúster, ejecute una prueba de migración tras error para comprobar que los nodos están funcionando correctamente.

 Sistemas operativos Windows

Preparación de un grupo de Microsoft Failover Cluster para un servidor virtual básico

Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster.

Antes de empezar

Utilice el programa Failover Cluster Manager en el sistema que es propietario del recurso de cinta o disco compartido para preparar su grupo de recursos. Inicialmente, el grupo debe contener solamente recursos de disco. Puede crear un grupo y mover recursos de disco a él. También puede optar por cambiar el nombre de un grupo de recursos existente que contenga sólo recursos de disco.

Cuando construya los grupos de recursos, tenga en cuenta los siguientes elementos:

- Asegúrese de que cada grupo de recursos tenga un nombre distintivo. No cambie los nombres una vez creado el grupo porque puede dañar la configuración.
- Asegúrese de que todos los nodos del clúster se encuentren en línea.
- Asegúrese de que el grupo esté en línea y sea propiedad del nodo donde se ha instalado la instancia de servidor inicial.

Procedimiento

Para preparar un grupo de recursos para la configuración de clúster, realice los siguientes pasos:

1. Abra el programa Failover Cluster Manager. Pulse el botón derecho sobre Servicios y aplicaciones y, a continuación, seleccione Más acciones > Crear aplicación o servicio vacío.
2. Pulse el botón derecho sobre Nuevo servicio o aplicación, seleccione Cambiar el nombre y elija un nombre nuevo para el grupo de recursos, como por ejemplo TSMGROUP.
3. Pulse el botón derecho sobre el grupo de recursos TSMGROUP y seleccione Añadir almacenamiento.
4. En el panel Añadir área de almacenamiento, seleccione el volumen o los volúmenes compartidos para IBM Spectrum Protect y pulse OK. Se muestra el grupo de recursos TSMGROUP, que contiene los volúmenes de disco que ha agregado.

 Sistemas operativos Windows

Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster

Instale el servidor de IBM Spectrum Protect en cada nodo del clúster que aloje un servidor en clúster de IBM Spectrum Protect.

Procedimiento

Siga estos pasos para cada nodo del clúster para instalar el servidor de IBM Spectrum Protect:

1. Inicie sesión con un ID de usuario de dominio o administrador. El usuario de dominio debe ser miembro del grupo de administradores del dominio.
2. Instale el servidor de IBM Spectrum Protect en un disco local en cada nodo. Utilice la misma letra de unidad de disco local para cada nodo.
3. Reinicie el sistema cuando finalice la instalación del servidor.


 Sistemas operativos Windows

Inicialización del servidor de IBM Spectrum Protect para un Microsoft Failover Cluster en el nodo primario

Después de instalar IBM Spectrum Protect en los nodos del clúster, debe inicializar el servidor en el nodo primario.

Procedimiento

1. Asegúrese de que todos los sistemas se reinicien después de la instalación. Compruebe que todos los sistemas se ejecuten correctamente.
2. Inicie sesión con un ID de usuario de dominio o administrador. El usuario de dominio debe estar en el mismo dominio que el servidor de IBM Spectrum Protect.
3. Abra el programa Failover Cluster Manager y verifique que los recursos están en línea y disponibles en el nodo primario.
4. Inicie el proceso de inicialización en el nodo primario del clúster. En el programa Failover Cluster Manager, verifique que el propietario del grupo de recursos sea el nodo primario del clúster.
5. En el menú Inicio, pulse Todos los programas > Servidor de IBM Spectrum Protect > Asistente de configuración.
6. Siga las instrucciones del asistente; pulse Siguiente para seguir los pasos del asistente. Cuando se le solicite el ID de usuario, escriba el nombre de la cuenta de dominio que desee asociar con el clúster.
7. Si se ha completado la inicialización, pulse Finalizado.

 Sistemas operativos Windows

Verificación de la configuración de IBM Spectrum Protect en un Microsoft Failover Cluster

Cuando termine de configurar IBM Spectrum Protect en un Microsoft Failover Cluster, puede revisar la ventana de resumen de Failover Cluster Manager. Verifique que la agrupación en clúster se haya completado correctamente y que el servidor de IBM Spectrum Protect se haya iniciado.

Procedimiento

Para verificar que la instancia del servidor de IBM Spectrum Protect en un Microsoft Failover Cluster se ha creado y configurado correctamente, realice los pasos siguientes:

1. En Failover Cluster Manager, seleccione la instancia del servidor. El nombre de red que ha configurado se muestra en el panel Nombre del servidor.
2. En el panel Otros recursos, confirme que se visualizan la instancia de servidor y el recurso de servidor de IBM® DB2.
3. Pulse con el botón derecho la instancia del servidor de IBM Spectrum Protect y seleccione Colocar este recurso en línea.

 Sistemas operativos Windows

Prueba de recuperación de errores para el clúster

Después de completar la configuración de clúster, ejecute una prueba de migración tras error para comprobar que los nodos están funcionando correctamente.

Procedimiento

1. Abra Failover Cluster Manager. En Other Resources, pulse con el botón derecho el recurso IBM Spectrum Protect Instance(x). Seleccione Bring this resource online.
2. Para probar la recuperación de errores, pulse con el botón derecho el grupo de recursos de clúster de IBM Spectrum Protect y seleccione Move this service or application to another node.
3. Compruebe que la recuperación de errores desde el segundo nodo al primero se realice satisfactoriamente.

Mantenimiento del entorno en clúster

Después configurar el clúster o los clústeres iniciales, las necesidades de mantenimiento son mínimas.

Compruebe regularmente las anotaciones de sucesos de Windows (preferiblemente a diario), para controlar la actividad de los nodos del clúster. Utilice el registro para comprobar si un nodo falla y necesita mantenimiento.

La siguiente lista de temas describe las situaciones que puedan afectar a la configuración o el formato del clúster después de que esté en funcionamiento.


-  **Migración de un servidor de IBM Spectrum Protect existente a un clúster**
El motivo de mover datos de cliente a un clúster es similar al motivo de agregar un servidor a un clúster. Desea aumentar la disponibilidad y la fiabilidad de los datos para todos los usuarios. Cuando el servidor forma parte del clúster, proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.
-  **Agregación de un servidor de IBM Spectrum Protect con copia de seguridad y restauración**
Si tiene recursos de hardware limitados, puede agregar un servidor de IBM Spectrum Protect ya existente a un clúster utilizando un procedimiento de copia de seguridad y restauración.
-  **Gestión de un servidor de IBM Spectrum Protect virtual en un clúster**
Para la mayoría de las tareas, puede administrar un servidor de IBM Spectrum Protect virtual igual que un servidor no de clúster. Para completar tareas como el inicio y detención del servidor o el movimiento de un grupo de recursos a otro nodo para completar el mantenimiento del sistema, debe utilizar la interfaz de Microsoft Cluster Administrator.
-  **Gestión de la recuperación de errores de cinta en un clúster**
Como parte de las tareas rutinarias, compruebe las anotaciones de sucesos para asegurarse de que la configuración funciona correctamente. Si un servidor falla, se registra el error. La anotación ofrece información sobre el motivo por el que se produjo la anomalía.
-  **Resolución de problemas con las anotaciones de clúster de IBM Spectrum Protect**
El DLL de recursos de clúster de IBM Spectrum Protect notifica sucesos y errores a las anotaciones de clúster. Las anotaciones de clúster son una herramienta útil de resolución de problemas. Cuando se activan estas anotaciones, registran las acciones de cada componente del servicio de clúster como el resultado de cada acción.

Migración de un servidor de IBM Spectrum Protect existente a un clúster

El motivo de mover datos de cliente a un clúster es similar al motivo de agregar un servidor a un clúster. Desea aumentar la disponibilidad y la fiabilidad de los datos para todos los usuarios. Cuando el servidor forma parte del clúster, proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.

Acerca de esta tarea

Para migrar un servidor de IBM Spectrum Protect existente a un clúster, puede mover los clientes o realizar un procedimiento de copia de seguridad o restauración. La opción depende principalmente de la disponibilidad y la capacidad de los otros sistemas de servidor IBM Spectrum Protect del sitio y de su familiaridad con el procedimiento de copia de seguridad y restauración.

-  **Movimiento de los clientes**
Si mueve clientes de un sistema de servidor de IBM Spectrum Protect no de clúster a otro en clúster, tendrá tiempo para migrar gradualmente los usuarios al nuevo sistema y no interrumpir los servicios. No obstante, debe tener el hardware necesario para ejecutar dos servidores de IBM Spectrum Protect simultáneamente.

Tareas relacionadas:

Instalación y actualización del servidor

Agregación de un servidor de IBM Spectrum Protect con copia de seguridad y restauración

Si tiene recursos de hardware limitados, puede agregar un servidor de IBM Spectrum Protect ya existente a un clúster utilizando un procedimiento de copia de seguridad y restauración.

Acerca de esta tarea

Por ejemplo, suponga que el único hardware que tiene son los dos sistemas de servidor que se van a agrupar en clúster. Y tiene previsto utilizar el sistema que está ejecutando actualmente el servidor de IBM Spectrum Protect como nodo. Complete este procedimiento para eliminar IBM Spectrum Protect del sistema y volver a instalarlo en el clúster:

Procedimiento

1. Realice una copia de seguridad de todas las agrupaciones de almacenamiento de disco en una agrupación de almacenamiento de copia.
2. Realice una copia de seguridad de la base de datos del servidor de IBM Spectrum Protect existente.
3. Instale y configure el clúster.
4. Restaure la base de datos en el servidor de IBM Spectrum Protect en clúster.
5. Restaure los volúmenes de agrupación de almacenamiento de disco de la agrupación de almacenamiento de copia.
6. Después de comprobar que todos los datos están en el servidor en clúster, elimine el servidor antiguo.

 Sistemas operativos Windows


Gestión de un servidor de IBM Spectrum Protect virtual en un clúster

Para la mayoría de las tareas, puede administrar un servidor de IBM Spectrum Protect virtual igual que un servidor no de clúster. Para completar tareas como el inicio y detención del servidor o el movimiento de un grupo de recursos a otro nodo para completar el mantenimiento del sistema, debe utilizar la interfaz de Microsoft Cluster Administrator.

Acerca de esta tarea

La interfaz de Microsoft Cluster Administrator está disponible a través del grupo de programas Herramientas administrativas. La interfaz es una vista detallada de la configuración del servidor virtual. La configuración del servidor virtual incluye detalles como, por ejemplo, los servidores de Windows físicos que componen el clúster y sus recursos, las conexiones de red y el estado. Visualice los componentes de una configuración de servidor virtual e inicie, detenga o migre tras error un servidor virtual utilizando esta interfaz. Gestione un servidor IBM Spectrum Protect virtual utilizando la interfaz de Microsoft Cluster Administrator para evitar fallos del servidor y mensajes de error. Por ejemplo, si utiliza el gestor de control de servicio de Windows para apagar el servidor, puede recibir mensajes de que el servidor ha fallado.

Es posible que desee mover un servidor IBM Spectrum Protect virtual cuando el servidor de Windows actúa como nodo primario y este servidor requiere mantenimiento de hardware o del sistema. Utilice la interfaz de Microsoft Cluster Administrator para mover la gestión del servidor IBM Spectrum Protect virtual a un nodo secundario hasta que se haya completado el mantenimiento.

 Sistemas operativos Windows

Gestión de la recuperación de errores de cinta en un clúster

Como parte de las tareas rutinarias, compruebe las anotaciones de sucesos para asegurarse de que la configuración funciona correctamente. Si un servidor falla, se registra el error. La anotación ofrece información sobre el motivo por el que se produjo la anomalía.

Acerca de esta tarea

A veces un nodo debe reincorporarse al clúster, por ejemplo:

- Cuando falla un nodo
- Cuando se agrega una nueva tarjeta de fibra de adaptador de bus de host (cambios de equipo)

Procedimiento

Realice las siguientes tareas para asegurarse de que un nodo pueda incorporarse satisfactoriamente al clúster:

- Actualice, si es necesario, la unidad y la biblioteca que utilizan la herramienta de clúster de IBM Spectrum Protect.
- Deje el servidor de IBM Spectrum Protect fuera de línea hasta que el nodo que ha fallado se reincorpore al clúster. Esta acción permite garantizar que el servidor de IBM Spectrum Protect que se ejecuta en el otro nodo no se vea afectado.

 Sistemas operativos Windows

Resolución de problemas con las anotaciones de clúster de IBM Spectrum Protect

El DLL de recursos de clúster de IBM Spectrum Protect notifica sucesos y errores a las anotaciones de clúster. Las anotaciones de clúster son una herramienta útil de resolución de problemas. Cuando se activan estas anotaciones, registran las acciones de cada componente del servicio de clúster como el resultado de cada acción.

En comparación con el registro de sucesos de Microsoft Windows, el registro de clúster es un registro completo de la actividad del clúster. Las anotaciones de clúster registran la actividad del servicio de clúster que se registra en las anotaciones de sucesos. Aunque las anotaciones de sucesos pueden indicarle un problema, las anotaciones de clúster le ayudan a resolverlo.

Las anotaciones de clúster están habilitadas de forma predeterminada en Windows. La salida se imprime como un archivo de registro en %SystemRoot%\Cluster. Para obtener más información, consulte la documentación de ayuda en línea de Windows.

Configuración de clientes para aplicaciones, máquinas virtuales y sistemas

El servidor protege los datos de los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Personalización de políticas
Los objetivos de una empresa en cuanto a la protección y conservación de los datos suelen definirlos los ejecutivos de la empresa, los asesores legales y otros cargos importantes. Las *políticas* son la forma de adaptar el funcionamiento de IBM Spectrum Protect a los objetivos de protección y conservación de datos de su empresa.

Adición de clientes

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

Acerca de esta tarea

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones de la sección Selección del software de cliente y planificación de la instalación.

2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de la sección Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de la sección Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones de la sección Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones de la sección Instalación y configuración de clientes.

Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

Acerca de esta tarea

La práctica preferida consiste en instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente, de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración de la documentación de producto para asegurarse de que se puedan ejecutar operaciones planificadas.

Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de copia de seguridad y archivado realiza la copia de seguridad y archivado de directorios y archivos desde los servidores de archivos y las estaciones de trabajo al almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none"> • Requisitos del cliente de archivado y copia de seguridad • Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux • Instalación del cliente de archivado y copia de seguridad de Windows
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM Software de base de datos de DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot para VMware • Instalación y actualización de IBM Spectrum Protect Snapshot para Windows
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection para IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se completen sin tener que concluir los servidores IBM Domino.	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se completen sin tener que concluir los servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server

Objetivo	Producto y descripción	Instrucciones de instalación
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de copia de seguridad y archivado se puede utilizar para realizar la copia de seguridad de los datos de DB2 en el servidor de IBM Spectrum Protect.	Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de copia de seguridad y archivado se puede utilizar para hacer una copia de seguridad de los datos de Informix en un servidor IBM Spectrum Protect.	Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect para bases de datos: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection para SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect para bases de datos: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2 • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales que están almacenadas en un servidor centralizado, para crear políticas de copia de seguridad y para restaurar máquinas virtuales o archivos individuales.</p> <p>Como alternativa, puede utilizar el cliente de copia de seguridad y archivado para hacer copias de seguridad y restaurar una máquina virtual VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> • Instalación de protección de datos para Microsoft Hyper-V • Instalación y actualización de Data Protection para VMware • Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

Acerca de esta tarea

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el período de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro del cliente, puede asignar un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activo*.

Cuando un cliente realiza una copia de seguridad o de archivado de un archivo, el archivo se enlaza a una clase de gestión del conjunto de políticas activas del dominio de políticas. Una *clase de gestión* es el conjunto principal de las reglas para gestionar datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo editable local en el sistema cliente y en un conjunto de opciones de cliente del servidor. Las opciones del conjunto de opciones de cliente del servidor pueden sustituir o añadirse a las opciones en el archivo de opciones de cliente local.

Procedimiento

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

Visualización de políticas

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

Procedimiento

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
 - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
Consejo: Para asegurarse de que se recuperan los datos tras un ataque de ransomware, aplique las directrices siguientes:
 - Asegúrese de que el valor de la columna Copia de seguridad sea de como mínimo 2. El valor preferido es 3, 4 o más.
 - Asegúrese de que el valor de la columna Mantener copias de seguridad extra esté en un mínimo de 14 días. El valor preferido son 30 días o más.
 - Asegúrese de que el valor de la columna Mantener archivos esté en un mínimo de 30 días.

Si el software IBM Spectrum Protect for Space Management está instalado en el cliente, asegúrese de realizar una copia de seguridad de los datos antes de migrarlos. En el mandato DEFINE MGMTCLASS o UPDATE MGMTCLASS, especifique MIGREQUIRESBKUP=YES. A continuación, siga las directrices de la sugerencia.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
 - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
 - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
 - c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

Edición de políticas

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
Añadir una clase de gestión	<ol style="list-style-type: none"> a. En la tabla Conjuntos de políticas, pulse +Clase de gestión. b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión. c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada. d. Pulse Añadir.
Suprimir una clase de gestión	<p>En la columna Clase de gestión, pulse -.</p> <p>Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.</p>
Establecer una clase de gestión como clase de gestión predeterminada	<p>En la columna Predeterminada para la clase de gestión, pulse el botón de selección.</p> <p>Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.</p>
Modificar una clase de gestión	<p>Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.</p>

6. Pulse Guardar.

Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:
 - a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
 - b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.
 - c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menús Centro de operaciones. Pulse Planificaciones.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
Modificar una planificación	<ol style="list-style-type: none">a. En la vista Planificaciones, seleccione la planificación y pulse Detalles.b. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas.c. Modifique los valores de la planificación y pulse Guardar.
Crear una planificación	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
 - a. En la página Visión general del Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.
 - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

Tareas relacionadas:

 Ajuste de la planificación para las operaciones diarias

Registro de clientes

Registre un cliente para asegurarse de que el cliente se puede conectar al servidor y que el servidor puede proteger los datos del cliente.

Antes de empezar

Determine si el cliente requiere un ID de usuario de administración con autoridad de propietario de cliente sobre el nodo del cliente. Para determinar qué clientes necesitan un ID de usuario de administración, consulte la nota técnica 7048963.

Restricción: Para algunos clientes, el nombre de nodo del cliente y el ID de usuario de administración deben coincidir. No puede autenticar estos clientes mediante el método de autenticación de protocolo de acceso Lightweight Directory Access Protocol que se introdujo en la versión V7.1.7. Para obtener detalles acerca de este método de autenticación, al que a veces se hace referencia como modo integrado, consulte Autenticación de los usuarios mediante una base de datos de Active Directory.

Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente requiere un ID de usuario de administración, registre al cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node
nombre_nodo contraseña
userid=nombre_nodo
```

donde *nombre_nodo* especifica el nombre del nodo y la *contraseña* especifica la contraseña del nodo. Si desea obtener más información al respecto, consulte el apartado Registro de un nodo.

- Si el cliente no necesita un ID de usuario de administración, registre al cliente mediante el Centro de operaciones asistente Añadir cliente. Realice los pasos siguientes:
 - a. En la barra de menús de Centro de operaciones, pulse Clientes.
 - b. En la tabla Clientes, pulse + Cliente.
 - c. Complete los pasos en el asistente Añadir cliente:
 - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de deduplicación de datos del lado del cliente, active la casilla de verificación Habilitar.
 - ii. En la ventana Configuración, copie los valores de opción TCPSERVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
 - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
 - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
 - v. Pulse Añadir cliente.

Referencia relacionada:

- [DECOMMISSION NODE \(Dejar fuera de servicio un nodo de cliente\)](#)
- [DECOMMISSION VM \(Dejar fuera de servicio una máquina virtual\)](#)
- [QUERY NODE \(Consultar nodos\)](#)
- [REMOVE REPLNODE \(Eliminar un nodo de cliente de la réplica\)](#)

Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:
 - o Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none">■ Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux■ Instalación del cliente de archivado y copia de seguridad de Windows Consejo: También puede actualizar los clientes existentes mediante el uso de Centro de operaciones. Para obtener las instrucciones, consulte Planificación de actualizaciones de cliente.
IBM Spectrum Protect para bases de datos	<ul style="list-style-type: none">■ Instalación de Data Protection for Oracle■ Instalación de Data Protection para SQL Server en Windows Server Core
IBM Spectrum Protect for Mail	<ul style="list-style-type: none">■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server

Software	Enlace a instrucciones
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> ■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux ■ Instalación y actualización de IBM Spectrum Protect Snapshot para VMware ■ Instalación y actualización de IBM Spectrum Protect Snapshot para Windows
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2 ■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> ■ Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux ■ Instalación del cliente de archivado y copia de seguridad de Windows
Si tiene previsto crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> ■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSERVERADDRESS, TCPSPORT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (Registro de clientes).
 - Para los clientes que están instalados en un sistema operativo AIX, Linux, Mac OS X u Oracle Solaris, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
 - Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt.

De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de cliente en el cliente. Siga las instrucciones del apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones de la sección Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones de la sección Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:
 - a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
 - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

Qué hacer a continuación

Si necesita cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones de Modificación del ámbito de una copia de seguridad de cliente.

Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

Acerca de esta tarea

El método preferido consiste en instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente, de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Mediante el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que se puedan ejecutar operaciones planificadas.

Si la empresa utiliza una herramienta de planificación de otro proveedor como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Por lo general, las herramientas de planificación de terceros inician los programas de cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

Procedimiento

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones correspondientes al sistema operativo que está instalado en el nodo cliente.

AIX y Oracle Solaris

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- Para permitir que el aceptador de cliente se inicie automáticamente después de un reinicio del sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```

Linux

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente iniciando una sesión con el ID de usuario `root` y emitiendo el mandato siguiente:

```
service dsmcad start
```

- Para permitir que el aceptador de cliente pueda iniciarse automáticamente después de un reinicio del sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

MAC OS X

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- c. Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- d. Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- e. Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

Windows

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- b. Consulte la información en la página Asistente del planificador y pulse Siguiente.
- c. En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- d. En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- e. Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- f. Complete la configuración paso a paso a través del asistente.
- g. Actualice el archivo de opciones de cliente, dsm.opt, y configure la opción passwordaccess como generate.
- h. Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- i. Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El aceptador de cliente inicia y detiene automáticamente el servicio de planificador según sea necesario.

Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

Antes de empezar

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores del archivo de opciones del cliente que ha obtenido durante dicho proceso. Puede utilizar los valores para especificar los puertos.

Acerca de esta tarea

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

Procedimiento

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción tcppport en el archivo de opciones de cliente. La opción tcppport del archivo de opciones de cliente debe coincidir con la opción TCPPOINT en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción `httpport` en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción `webports` en el archivo de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción `tcpadminport` de cliente debe coincidir con el valor de la opción de servidor `TCPADMINPORT`. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.

Planificación de actualizaciones de cliente

Permite planificar la instalación automática de actualizaciones de software para clientes de archivo de copia de seguridad de IBM Spectrum Protect. Esta función también se denomina en ocasiones *despliegue del cliente*.

Antes de empezar

Para planificar las actualizaciones de cliente utilizando el Centro de operaciones, configure el entorno para que cumpla los siguientes requisitos:

Requisitos del servidor

Los servidores IBM Spectrum Protect deben cumplir los siguientes requisitos:

- IBM Spectrum Protect V8.1.3 o posterior debe estar instalado en los servidores concentrador y spoke.
- Los servidores concentrador y spoke deben tener especificadas una dirección de nivel superior y una dirección de nivel inferior. Puede configurar estos parámetros utilizando los mandatos `SET SERVERHLADDRESS` y `SET SERVERLLADDRESS`.
- El servidor concentrador debe tener especificada una contraseña de servidor. Puede configurar este parámetro utilizando el mandato `SET SERVERPASSWORD`.
- El servidor concentrador debe tener estar definido para los servidores spoke. Esta definición se realiza automáticamente cuando se añaden los servidores spoke al Centro de operaciones. Para definir el servidor concentrador, emita el mandato `DEFINE SERVER` y utilice la segunda opción de sintaxis de la documentación de mandatos. Por ejemplo, puede emitir el siguiente mandato en cada servidor spoke:

```
DEFINE SERVER nombre_concentrador SERVERPASSWORD=contraseña_concentrador  
HLA=IP_concentrador  
LLA=puerto_concentrador SSL=NO SESSIONSECURITY=TRANSITIONAL
```

donde las variables representan los siguientes parámetros del servidor concentrador: *nombre_concentrador* es el nombre del servidor, *contraseña_concentrador* es la contraseña del servidor, *IP_concentrador* es la dirección de nivel superior y *puerto_concentrador* es la dirección de nivel inferior.

- El puerto que se especifica con la opción de servidor `RESTHTTPSPORT` debe estar abierto para permitir la comunicación segura entre el Centro de operaciones y el servidor concentrador. El número de puerto predeterminado es 8443.
- Los servidores spoke deben tener una agrupación de almacenamiento de contenedores de directorio o una agrupación de almacenamiento `FILE` disponible para almacenar paquetes de actualización. El Centro de operaciones selecciona automáticamente una agrupación de almacenamiento para su uso.

Requisitos de cliente

Los clientes de archivo de copia de seguridad de IBM Spectrum Protect que tiene previsto actualizar utilizando el Centro de operaciones debe cumplir los siguientes requisitos:

- La opción `passwordaccess` debe estar establecida en `generate`.
- La opción de cliente `autodeploy` debe estar establecida en un valor que no sea `no`. Para obtener más información sobre esta opción, consulte `Autodeploy`.
- Los clientes de archivo de copia de seguridad de 32 bits no se soportan. Si se detecta un cliente de archivo de copia de seguridad de 32 bits en un sistema operativo de 64 bits, el cliente se actualizará a la versión de 64 bits.
- El planificador de cliente debe estar en ejecución.
- El sistema cliente debe estar en ejecución y el cliente se debe haber conectado con el servidor IBM Spectrum Protect al menos una vez.

Los clientes Microsoft Windows deben cumplir los siguientes requisitos adicionales:

- El planificador de cliente se debe iniciar como un servicio de Windows y no desde la línea de mandatos. Para reducir al mínimo las posibilidades de reinicio, el servicio de planificador se cierra antes de instalar el cliente nuevo y se reinicia

después de la instalación. Si el planificador no se está ejecutando como un servicio de Windows, será necesario reiniciar cuando se actualice el cliente.

- La versión de la línea de mandatos del programa de utilidad de registro de Windows (reg.exe) es necesaria. Esta herramienta se suele instalar como parte de la instalación del sistema operativo en sistemas operativos Windows soportados.

Acerca de esta tarea

Puede utilizar el Centro de operaciones para actualizar de forma simultánea varios clientes a una hora planificada.

Los paquetes de actualización se descargan automáticamente en el servidor concentrador, se importan y se replican a los servidores spoke. Cuando se ejecuta una planificación de actualización, los archivos del paquete de instalación se copian en el sistema cliente y el cliente se actualiza a la versión de software especificada.

Restricciones:

- Sólo puede planificar actualizaciones de cliente de archivo de copia de seguridad. Las actualizaciones para los otros tipos de cliente se deben instalar de forma manual.
- El software del cliente de archivado de copia de seguridad no puede ser actualizado por distintos gestores de despliegue de IBM Spectrum Protect a la vez.
- El entorno de servicios de clúster de Microsoft Windows no se soporta.
- No planifique despliegues de clientes automáticos en sistemas con algunas de las siguientes aplicaciones instaladas:
 - IBM Spectrum Protect for Virtual Environments
 - IBM Spectrum Protect para bases de datos
 - IBM Spectrum Protect for Mail
 - IBM Spectrum Protect for Enterprise Resource Planning
- Para gestionar actualizaciones, el Centro de operaciones crea objetos de política, con clases de dispositivos, agrupaciones de almacenamiento y dominios, en los servidores concentrador y spoke. Estos objetos siguen la convención de nomenclatura siguiente: `IBM_DEPLOY_CLIENTS`. Para evitar interferencias con otras operaciones de actualización, no modifique estos objetos.
- Si ha configurado manualmente el despliegue del cliente para un servidor de una versión anterior, suprima los objetos de política definidos antes de planificar las actualizaciones de cliente utilizando el Centro de operaciones.
- Sólo puede planificar actualizaciones en clientes existentes. No puede utilizar el Centro de operaciones para instalar un cliente nuevo.

Para obtener información sobre la instalación manual de software de cliente de archivo de copia de seguridad, consulte Instalación de clientes de archivo de copia de seguridad de IBM Spectrum Protect en la documentación de IBM Spectrum Protect.

Para obtener información sobre la instalación de otros clientes IBM Spectrum Protect, consulte el apartado Suites de producto y productos relacionados.

Procedimiento

1. En la barra de menú del Centro de operaciones, pulse Actualizaciones > Clientes. Se abre la página Actualizaciones de cliente de archivado y copia de seguridad.
2. Utilice la información de la página para determinar el release que se debe instalar, pulse Planificar actualización y complete los pasos del asistente.

Qué hacer a continuación

Para supervisar, cancelar o volver a planificar actualizaciones, pulse Actualizaciones > Planificadas.

Para diagnosticar y solucionar problemas, consulte la nota técnica 2007749.

Información relacionada:

SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)
SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)
SET SERVERPASSWORD (Establecer contraseña de servidor)
DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)
RESTHTTPSPORT

Personalización de políticas

Los objetivos de una empresa en cuanto a la protección y conservación de los datos suelen definirlos los ejecutivos de la empresa, los asesores legales y otros cargos importantes. Las *políticas* son la forma de adaptar el funcionamiento de IBM Spectrum Protect a los objetivos de protección y conservación de datos de su empresa.

Acerca de esta tarea

Para gestionar de forma automática la protección y conservación de datos, defina políticas, que son las reglas que se configuran en el servidor. Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y al periodo de tiempo que los datos se retienen y están disponibles para ser restaurados por los clientes. Personalice las políticas para cumplir con los objetivos de protección de datos de su organización.

Puede elegir la política que gestiona los datos de un cliente, asignando al cliente a un dominio de políticas. Los clientes de diferentes tipos tienen diferentes requisitos de retención y normalmente es necesario personalizar y crear políticas.

Cuando se instala un servidor, este tiene de forma predeterminada una política en un dominio de políticas. Puede personalizar la política y crear sus propias políticas.

- **Conceptos de políticas**
La política de un cliente específico se determina mediante los valores del dominio de políticas al que se ha añadido el cliente.
- **Personalización de una política**
Puede personalizar las políticas existentes para que cumplan los requisitos de retención de datos nuevos o revisados de la organización. La modificación de un dominio de políticas o la copia de un dominio de políticas existente es una forma habitual de personalizar una política.
- **Creación de una política copiando una política existente**
Puede crear nuevas políticas copiando una política existente y, a continuación, actualizando las partes que desea cambiar.
- **Creación de un dominio de políticas**
Es posible que desee crear un nuevo dominio de políticas para cada tipo de cliente que esté protegido mediante el servidor. Es posible que también desee dividir las responsabilidades de los clientes entre varios administradores concediéndoles autorización para dominios de políticas específicos.
- **Control de las operaciones de cliente mediante conjuntos de opciones de cliente**
Puede utilizar conjuntos de opciones de cliente para controlar de forma centralizada las opciones de proceso que utilizan los clientes para operaciones, tales como una copia de seguridad. Los conjuntos de opciones de cliente garantizan que los datos estén protegidos de forma coherente de acuerdo con sus requisitos. Un conjunto de opciones de cliente pueden reemplazar las opciones en un archivo de opciones de cliente y añadir opciones que podrían no estar en un archivo de opciones del cliente local.

Conceptos de políticas

La política de un cliente específico se determina mediante los valores del dominio de políticas al que se ha añadido el cliente.

Durante el proceso de registro del cliente, puede asignar un cliente a un *dominio de políticas*. La política de cada cliente se determina mediante las reglas del dominio de políticas al que se ha asignado al cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activo*.

Cuando un cliente realiza una copia de seguridad o de archivado de un archivo, el archivo se enlaza a una clase de gestión del conjunto de políticas activas del dominio de políticas. Una *clase de gestión* es el conjunto principal de las reglas para gestionar datos de cliente. Las operaciones de copia de seguridad y archivado del cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas, al menos que personalice la política.

Se puede personalizar una política definiendo más clases de gestión en el conjunto de políticas, activando el conjunto y asignando el uso de las nuevas clases de gestión mediante opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo editable local en el sistema cliente y en un conjunto de opciones de cliente del servidor. Las opciones del conjunto de opciones de cliente del servidor pueden sustituir o añadirse a las opciones en el archivo de opciones de cliente local.

El servidor utiliza la política de las clases de gestión para gestionar los archivos basándose en si hay versiones de archivos activas o inactivas. La copia de seguridad o la copia archivada más reciente de un archivo es la *versión activa*. Las versiones activas no se suprimen nunca del almacenamiento del servidor.

Las versiones de copia de seguridad que no sean la versión más reciente se denominan *versiones inactivas*. Una versión activa de un archivo pasa a estar inactiva cuando se produce uno de los sucesos siguientes:

- Se ha vuelto a realizar una copia de seguridad del archivo, lo que ha creado una versión más reciente del archivo en el almacenamiento del servidor.
- Se ha suprimido el archivo en el almacenamiento del nodo cliente y, a continuación, se ha ejecutado una operación de copia de seguridad incremental. Una *copia de seguridad incremental*, la operación de copia de seguridad más frecuente para un cliente, solo realiza una copia de seguridad de los archivos que se han modificado desde la última copia de seguridad.

Los valores de la clase de gestión que está vinculada a un archivo determinan durante cuánto tiempo y cuántas versiones inactivas de los archivos se conservarán.

El *proceso de caducidad* utiliza políticas para determinar cuándo dejarán de necesitarse los archivos, es decir, cuándo caducarán las versiones. El proceso de caducidad en el servidor aplica las políticas que ha definido para la retención de datos y debe asegurarse de que planifica la caducidad de modo que se ejecute con regularidad. Por ejemplo, si tiene una política que indica que se conserven sólo cuatro versiones de un archivo, caducará la quinta copia, que es la más antigua. Durante el proceso de caducidad, el servidor elimina de la base de datos las entradas de versiones caducadas, lo cual suprime de forma efectiva las versiones del almacenamiento del servidor.

- Retención y caducidad de las versiones de copia de seguridad

Es importante tener varias versiones de las copias de seguridad de archivos ya que los usuarios actualizan de forma continuada los archivos y es posible que necesiten restaurar un archivo en diferentes puntos en el tiempo. Los valores de las políticas controlan las versiones de copia de seguridad que retiene el servidor en el almacenamiento del servidor y afectan a lo que los usuarios pueden restaurar.

- Activación de las políticas después de las actualizaciones

Cuando realiza actualizaciones en la política, las actualizaciones no entran en vigor hasta que activa el conjunto de políticas que ha actualizado.

Conceptos relacionados:

 Copia de seguridad incremental completa y copia de seguridad incremental parcial

Retención y caducidad de las versiones de copia de seguridad

Es importante tener varias versiones de las copias de seguridad de archivos ya que los usuarios actualizan de forma continuada los archivos y es posible que necesiten restaurar un archivo en diferentes puntos en el tiempo. Los valores de las políticas controlan las versiones de copia de seguridad que retiene el servidor en el almacenamiento del servidor y afectan a lo que los usuarios pueden restaurar.

Puede especificar las versiones que retiene el servidor en el almacenamiento del servidor con los valores de la clase de gestión:

- Especifique el número de días que se conservarán las versiones de copia de seguridad.

Especifique el número de días que se han de conservar las versiones de copia de seguridad con valores en el Centro de operaciones:

- Mantener copias de seguridad extra, que es el número de días que se han de conservar las versiones de copia de seguridad inactivas. Los días se cuentan a partir del día en que las versiones pasan a estar inactivas.

Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro RETEXTRA.

Consejo: Para asegurarse de que los archivos se puedan recuperar tras un incidente de malware, como un ataque de ransomware, especifique un valor de como mínimo 14 días. El valor preferido es 30 días o más.

- Mantener copias de seguridad suprimidas, que es el número de días que se ha de conservar la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente.

Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro RETONLY.

Consejo: Para asegurarse de que los archivos se puedan recuperar tras un incidente de malware, como un ataque de ransomware, especifique un valor de como mínimo 30 días.

- Especifique el número de versiones para conservar.

Especifique el número de versiones de copia de seguridad para conservar con valores en el Centro de operaciones:

- Copias de seguridad, que es el número de versiones que se ha de conservar de un archivo que todavía existe en el sistema de archivos del cliente.

Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro VEREXISTS.

Consejo: Para asegurarse de que los archivos se puedan recuperar tras un incidente de malware, especifique un valor de como mínimo 2. Se prefieren los valores 3, 4 o más.

- Copias de seguridad suprimidas, que es el número de versiones para conservar de un archivo que se ha suprimido del sistema de archivos del cliente.

Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro VERDELETED.

- Especifique una combinación del número de versiones y el número de días que se conservarán.

Los valores interactúan para determinar las versiones de copia de seguridad que retiene el servidor. Asegúrese de que comprende qué valores tienen prioridad y qué interacciones se llevan a cabo:

- Cuando el número de versiones de copia de seguridad inactivas excede el número en los valores Copias de seguridad y Copias de seguridad suprimidas, la versión más antigua caduca y el servidor suprime el archivo de la base de datos la próxima vez que se ejecuta el proceso de caducidad.

- El número de versiones inactivas que el servidor conserva también está afectado por el valor de Mantener copias de seguridad extra. Las versiones inactivas caducan cuando el número de días que han permanecido inactivas excede el valor especificado para retener versiones adicionales, aunque no se supere el número de versiones.
- Caducidad de archivos y procesamiento de la caducidad

Los archivos caducan cuando superan el criterio de retención que se ha especificado en la política. El proceso de caducidad en el servidor elimina los archivos caducados de la base de datos del servidor y los archivos suprimidos del almacenamiento del servidor.
- Ejemplo: Retención cuando una política utiliza solo controles temporales

La forma más sencilla de gestionar la retención de datos es utilizar únicamente controles de política basados en el tiempo. Con controles basados en el tiempo únicamente en la política, las versiones de archivos se conservan en función de los días transcurridos desde que las versiones han pasado a estar inactivas.
- Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión

El uso de los controles de versión y de tiempo en una política ofrece una mayor flexibilidad en la gestión de la retención de datos, pero supone también más complejidad. Para comprender las interacciones entre los controles, revise ejemplos de políticas y sus efectos en la retención de las versiones de copia de seguridad de un archivo durante un mes.
- Interacciones entre configuraciones de política

Las configuraciones basadas en el tiempo y basadas en las versiones interactúan cuando se utilizan juntas en una clase de gestión de una política. La frecuencia de las copias de seguridad de cliente también afecta a las versiones de copia de seguridad que se almacenan para un cliente.

Caducidad de archivos y procesamiento de la caducidad

Los archivos caducan cuando superan el criterio de retención que se ha especificado en la política. El proceso de caducidad en el servidor elimina los archivos caducados de la base de datos del servidor y los archivos suprimidos del almacenamiento del servidor.

Los archivos caducan en las condiciones siguientes:

- Los usuarios suprimen espacios de archivos de los nodos cliente.
- Los usuarios hacen caducar archivos mediante el mandato EXPIRE en el cliente
- Una versión de copia de seguridad de un archivo supera el criterio de retención de copias de seguridad (el periodo de tiempo en que se conserva un archivo y el número de versiones inactivas de un archivo que se conservan)
- Un archivo de copia archivada supera el criterio de tiempo de retención para los archivos de copia archivada (el periodo de tiempo en que se conservan las copias archivadas).
- Un conjunto de copias de seguridad excede el tiempo de retención que tiene especificado para el conjunto de copias de seguridad.

El servidor suprime los archivos caducados de la base de datos del servidor sólo durante el proceso de caducidad. Una vez que los archivos caducados se suprimen de la base de datos, el servidor puede volver a utilizar el espacio en las agrupaciones de almacenamiento ocupado por los archivos caducados. Asegúrese de que el proceso de caducidad se ejecuta periódicamente para que el servidor pueda volver a utilizar espacio.

Restricciones relativas al proceso de caducidad

El uso de algunas funciones afecta al proceso de caducidad.

Réplica


Si utiliza políticas distintas en los servidores de origen y de destino, los archivos marcados para una caducidad inmediata en el servidor de réplica fuente no se suprimen hasta que se repliquen al servidor de réplica de destino. Si no utiliza políticas distintas, los archivos marcados para una caducidad inmediata en el servidor de réplica fuente se suprimen inmediatamente.

Para el servidor de réplica de destino, si los archivos se marcan como caducados, se suprimen cuando el servidor de réplica de destino ejecuta el procesamiento de la caducidad.

Retención basada en sucesos para datos de archivado

Una copia archivada no puede optar a la caducidad si existe una retención de supresión asociada. Si un archivo no está retenido, se gestionará según el proceso de caducidad existente.

Tareas relacionadas:

 Retención y liberación de la caducidad/supresión

Ejemplo: Retención cuando una política utiliza solo controles temporales

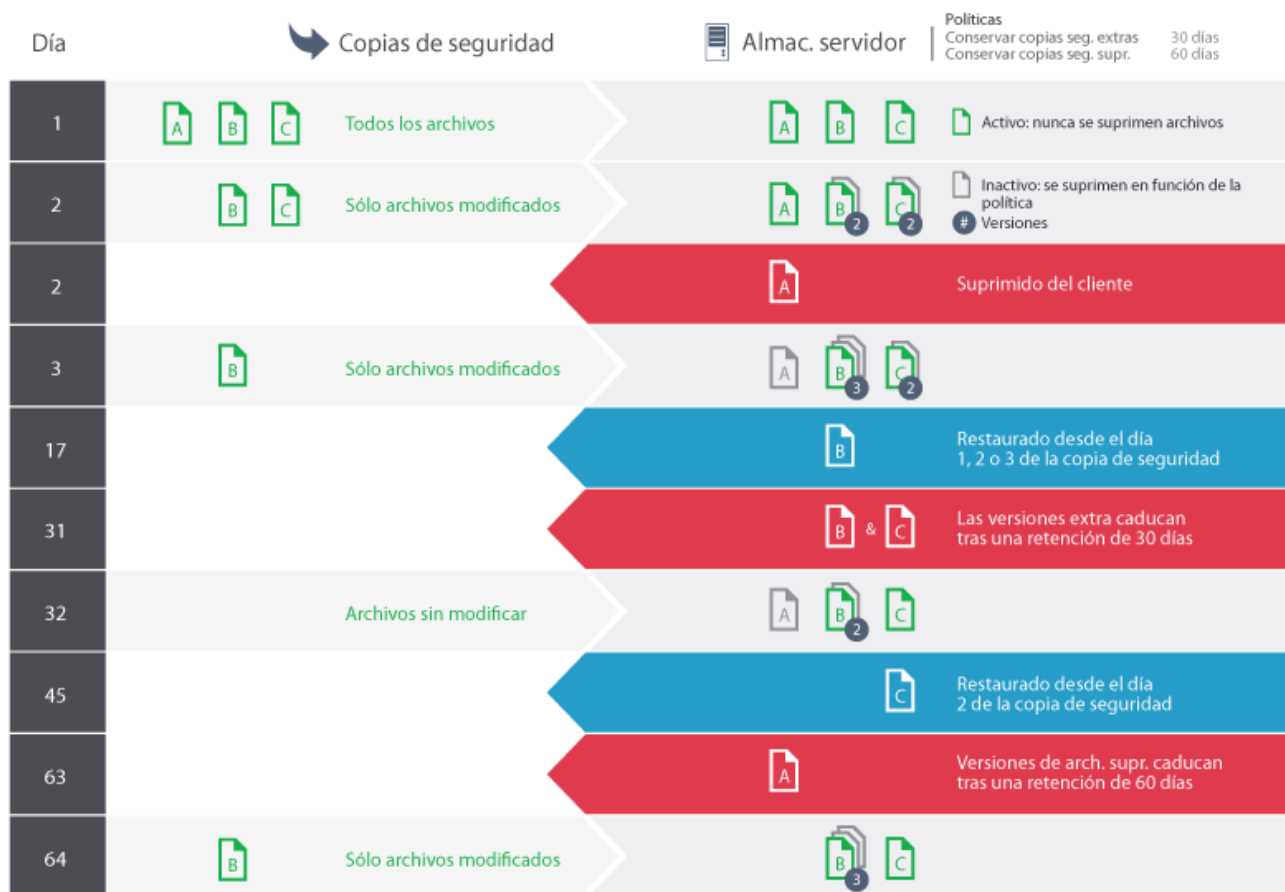
La forma más sencilla de gestionar la retención de datos es utilizar únicamente controles de política basados en el tiempo. Con controles basados en el tiempo únicamente en la política, las versiones de archivos se conservan en función de los días transcurridos desde que las versiones han pasado a estar inactivas.

En el caso de una política basada únicamente en el tiempo, utilice controles Mantener copias de seguridad extra y Mantener copias de seguridad suprimidas. Este tipo de política no limita el número de versiones de archivos. Si los clientes deben realizar copias de seguridad con frecuencia, asegúrese de que el almacenamiento del servidor pueda manejar el número potencial de versiones de archivos.

La siguiente figura muestra cómo el servidor maneja los archivos a lo largo del tiempo de un cliente que realiza copias de seguridad incrementales diariamente.

En este ejemplo, la política tiene las siguientes características:

- La versión más reciente de un archivo siempre se retiene mientras exista el archivo en el sistema del cliente. La versión más reciente del archivo es la versión activa. Esta característica forma parte de cada política en el servidor.
- Mantener copias de seguridad extra se establece en 30 días. Cuando se realiza una copia de seguridad más reciente, una versión del archivo pasa a estar inactiva y se conserva en el almacenamiento del servidor durante 30 días.
- Mantener copias de seguridad suprimidas se establece en 60 días. Cuando se suprime un archivo del sistema cliente, todas las versiones del archivo que se encuentran en el almacenamiento del servidor pasan a estar inactivas. Estas versiones inactivas se conservan durante 60 días después de que las versiones de archivo pasan a estar inactivas.



Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión

El uso de los controles de versión y de tiempo en una política ofrece una mayor flexibilidad en la gestión de la retención de datos, pero supone también más complejidad. Para comprender las interacciones entre los controles, revise ejemplos de políticas y sus efectos en la retención de las versiones de copia de seguridad de un archivo durante un mes.

Consulte los apartados Tabla 1 y Figura 1. Un cliente realiza una copia de seguridad del archivo REPORT.TXT cuatro veces en un mes, desde el 23 de marzo hasta el 23 de abril. Los valores del grupo de copias de seguridad de la clase de gestión a la que está enlazado el archivo REPORT.TXT determinan cómo maneja el servidor estas versiones de copia de seguridad. Tabla 2 muestra cómo los diferentes valores de grupo de copia puede afectar a las versiones, a partir del 24 de abril (un día después de la última copia de seguridad).

Tabla 1. Estado de las versiones de copia de seguridad de REPORT.TXT a partir del 24 de abril

Versión	Fecha de creación	Días desde que la versión está inactiva
Activa	23 de abril	(no se aplica)
Inactiva 1	13 de abril	1 (desde el 23 de abril)
Inactiva 2	31 de marzo	11 (desde el 13 de abril)
Inactiva 3	23 de marzo	24 (desde el 31 de marzo)

Figura 1. Versiones activas e inactivas de REPORT.TXT

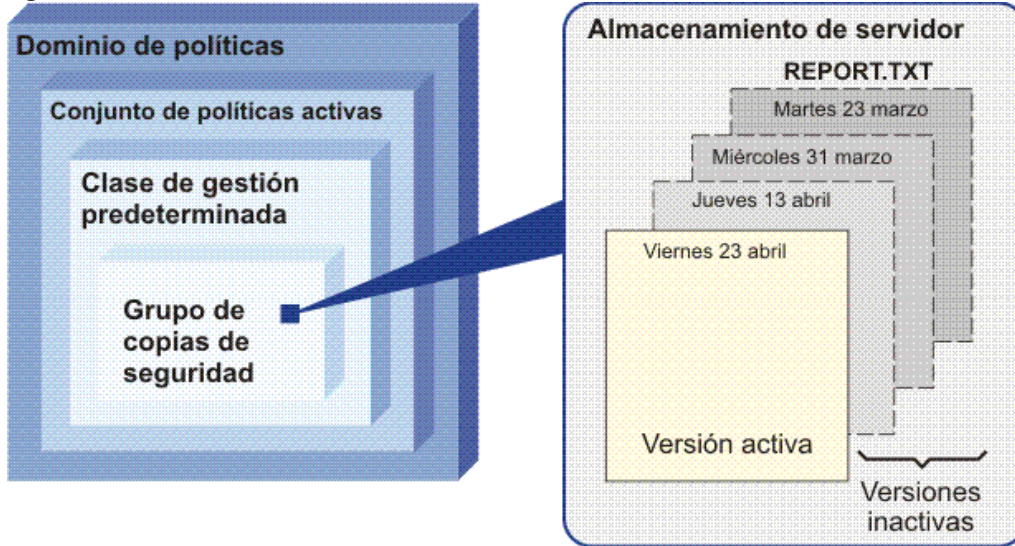


Tabla 2. Efectos de la política sobre la retención de versiones de copia de seguridad de REPORT.TXT a partir del 24 de abril

Copias de seguridad	Copias de seguridad suprimidas	Mantener copias de seguridad extra	Mantener copias de seguridad suprimidas	Resultado
4 versiones	2 versiones	60 días	180 días	<p>Los valores de Copias de seguridad y de Mantener copias de seguridad extra controlan la caducidad de las versiones. La versión creada el 23 de marzo se retiene hasta que se vuelve a realizar una copia de seguridad del archivo (lo que crea una cuarta versión inactiva) o hasta que esta versión permanece inactiva durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el sistema de archivos del cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del cliente. A partir de este punto, los valores de Copias de seguridad suprimidas y de Mantener copias de seguridad suprimidas también tienen un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan). La versión del 13 de abril caduca cuando permanece inactiva durante 60 días (el 23 de junio). El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>

Copias de seguridad	Copias de seguridad suprimidas	Mantener copias de seguridad extra	Mantener copias de seguridad suprimidas	Resultado
Número ilimitado	2 versiones	60 días	180 días	<p>El valor de Mantener copias de seguridad extra controla la caducidad de las versiones. Las versiones inactivas (no la última versión restante) caducan cuando permanecen inactivas durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del cliente. A partir de este punto, los valores de Copias de seguridad suprimidas y de Mantener copias de seguridad suprimidas también tienen un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan) porque sólo se permiten dos versiones. La versión del 13 de abril caduca cuando permanece inactiva durante 60 días (el 22 de junio). El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>
Número ilimitado	Número ilimitado	60 días	180 días	<p>El valor de Mantener copias de seguridad extra controla la caducidad de las versiones. El servidor no hace caducar las versiones inactivas en función del número máximo de copias de seguridad. Las versiones inactivas (no la última versión restante) caducan cuando permanecen inactivas durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del nodo de cliente. A partir de este punto, el valor de Mantener copias de seguridad suprimidas también tiene un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Tres de las cuatro versiones caducan después de estar inactivas cada una de ellas durante 60 días. El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>
4 versiones	2 versiones	Número ilimitado	Número ilimitado	<p>El valor de Copias de seguridad controla la caducidad de las versiones hasta que un usuario suprime el archivo del nodo cliente. El servidor no caduca las versiones inactivas en función de la antigüedad.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del nodo de cliente. A partir de este punto, el valor de Copias de seguridad suprimidas controla la caducidad. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan) porque sólo se permiten dos versiones. El servidor conserva las dos versiones inactivas restantes de forma indefinida.</p>

Conceptos relacionados:

 Copia de seguridad incremental completa y copia de seguridad incremental parcial

Interacciones entre configuraciones de política

Las configuraciones basadas en el tiempo y basadas en las versiones interactúan cuando se utilizan juntas en una clase de gestión de una política. La frecuencia de las copias de seguridad de cliente también afecta a las versiones de copia de seguridad que se almacenan para un cliente.

Para un sistema cliente que debe realizar una copia de seguridad de dos veces al día, tenga en cuenta los efectos de las siguientes opciones de política en un archivo que cambia frecuentemente:

- Establezca Mantener copias de seguridad extra en 30 días. Establezca Copias de seguridad a Sin límite para que la política no limite el número de versiones. Después de 30 días, el servidor podría tener 60 versiones con copia de seguridad del archivo si este cambia entre cada una de las dos copias de seguridad diarias. El cliente puede elegir restaurar cualquiera de los 60 versiones de los últimos 30 días.

- Establezca Mantener copias de seguridad extra en Sin límite, y Copias de seguridad en 30 versiones. Si el archivo cambia entre cada una de las dos operaciones de copia de seguridad diarias, el servidor tendrá 30 versiones con copia de seguridad después de 15 días. Después de 30 días, el servidor seguirá teniendo solo 30 versiones con copia de seguridad debido al límite del número de versiones. Si el archivo continúa cambiando entre cada una de las dos operaciones de copia de seguridad diarias, las versiones con copia de seguridad pueden ser solo de los últimos 15 días. El cliente puede optar por restaurar una de las 30 versiones, que podrían tener una antigüedad no superior a 15 días.

Los ejemplos muestran que si las versiones con copia de seguridad deben estar disponibles durante un determinado número de días, la forma más sencilla de implementar ese requisito es utilizar una política basada en el tiempo. Establezca Mantener copias de seguridad extra en el número de días específico y Copias de seguridad como Sin límite.

El efecto del valor Sin límite en la configuración de política varía en función de cómo se hayan configurado otros controles de política:

Mantener copias de seguridad extra

Si especifica Sin límite, se eliminarán las versiones con copia de seguridad inactivas en función de las configuraciones Copias de seguridad o Copias de seguridad suprimidas.

Para permitir que los nodos de cliente restauren los archivos a un instante específico, establezca Copias de seguridad o Copias de seguridad suprimidas en Número ilimitado. Establezca el valor de Mantener copias de seguridad extra en el número de días que, según sus previsiones, los clientes pueden necesitar que las versiones de los archivos estén disponibles para realizar una posible restauración a un instante específico. Por ejemplo, para permitir que los clientes restauren archivos a partir de un instante específico de 60 días de antigüedad, establezca Mantener copias de seguridad extra en 60.

Mantener copias de seguridad suprimidas

Si especifica Sin límite, la última versión se conserva de forma permanente salvo que un usuario o un administrador eliminen el archivo del almacenamiento del servidor.

Copias de seguridad

El establecimiento de la configuración como Sin límite puede suponer un incremento del almacenamiento, si bien puede ser necesario especificar este valor en algunas situaciones. Por ejemplo, para permitir que los nodos cliente restauren archivos a un instante específico, establezca el valor de Copias de seguridad en Número ilimitado. Si no establece un límite para las versiones, se asegura de que el servidor retenga las versiones en función del valor de Mantener copias de seguridad extra.

Copias de seguridad suprimidas

El establecimiento de la configuración como Sin límite puede suponer un incremento del almacenamiento, si bien puede ser necesario especificar este valor en algunas situaciones. Por ejemplo, establezca el valor de Copias de seguridad suprimidas en Número ilimitado para que los clientes puedan restaurar los archivos en un instante específico. Si no establece un límite para las versiones, se asegura de que el servidor retenga las versiones en función del valor de Mantener copias de seguridad extra.

Referencia cruzada de los campos y parámetros de mandatos de servidor de Centro de operaciones

La tabla siguiente muestra los campos Centro de operaciones con el parámetro equivalente para utilizar con el mandato `DEFINE COPYGROUP TYPE=BACKUP`.

Nombre de campo en las vistas de Centro de operaciones	Parámetro para utilizar con el mandato <code>DEFINE COPYGROUP TYPE=BACKUP</code>
Mantener copias de seguridad extra	RETEXTRA
Mantener copias de seguridad suprimidas	RETONLY
Copias de seguridad	VEREXISTS
Copias de seguridad suprimidas	VERDELETED

Activación de las políticas después de las actualizaciones

Cuando realiza actualizaciones en la política, las actualizaciones no entran en vigor hasta que activa el conjunto de políticas que ha actualizado.

La activación del conjunto de políticas activa las actualizaciones que ha realizado. Por ejemplo, los siguientes tipos de actualización entran en vigor después de que activa el conjunto de políticas:

- Define un nuevo dominio de políticas con un conjunto de políticas y una o varias clases de gestión

- Añade una clase de gestión a un conjunto de políticas
- Cambia los valores de retención de copias de seguridad en una clase de gestión existente

Validación del conjunto de políticas antes de la activación

En el Centro de operaciones, la validación no es un paso independiente. Si utiliza mandatos, la validación es un mandato opcional que le permite previsualizar el efecto de activar un conjunto de políticas modificado. Cuando valida un conjunto de políticas, el servidor informa acerca de las condiciones que pueden producir problemas si se activa el conjunto de políticas.

La validación no se puede ejecutar si el conjunto de políticas no contiene una clase de gestión predeterminada. La validación genera mensajes de aviso si existe alguna de las condiciones que se muestran en Tabla 1.

Tabla 1. Condiciones que generan avisos durante la validación de conjuntos de políticas

Condición	Razón del aviso
Los destinos de almacenamiento especificados para las operaciones de copia de seguridad, archivado o migración no están definidos en agrupaciones de almacenamiento.	Debe haber una agrupación de almacenamiento antes de que pueda especificarla como destino.
Un destino de almacenamiento especificado para operaciones de copia de seguridad, archivado o migración es una agrupación de almacenamiento de copias o una agrupación de datos activos.	El destino de almacenamiento debe encontrarse en una agrupación primaria.
La clase de gestión predeterminada no contiene valores de copia de seguridad o archivado.	Si la clase de gestión predeterminada no contiene valores de copias de seguridad o de archivado, no se hará una copia de seguridad ni una copia archivada de los archivos enlazados a la clase de gestión predeterminada.
El conjunto de políticas activas actual da nombre a una clase de gestión que no está definida en el conjunto de políticas que se está validando.	<p>Cuando los usuarios hacen copia de seguridad de archivos que están vinculados con una clase de gestión que ya no existe en el conjunto de políticas activas, las versiones de copia de seguridad se vuelven a vincular con la clase de gestión predeterminada.</p> <p>Cuando la clase de gestión con la que está vinculada una copia archivada ya no existe y la clase de gestión predeterminada no contiene valores de archivado, el servidor utiliza el período de gracia de retención de archivado para gestionar la retención de la copia archivada.</p> <p>El período de gracia de retención de archivado se establece para un dominio de políticas y dicho valor sólo se utiliza cuando ningún otro valor de política está disponible para gestionar una copia archivada.</p>
El conjunto de políticas activas actual contiene los valores de copia que no están definidos en el conjunto de políticas que se está validando.	<p>Cuando un cliente realiza una copia de seguridad de un archivo y la clase de gestión con la que está enlazado el archivo ya no contiene valores de copia de seguridad, las versiones de copia de seguridad las gestiona la clase de gestión predeterminada.</p> <p>Si la clase de gestión predeterminada no contiene ninguna configuración de copia de seguridad, el servidor utiliza el período de gracia de retención de copia de seguridad para gestionar las versiones de archivo. Sin embargo, no se realiza una copia de seguridad del archivo en la siguiente operación de copia de seguridad.</p> <p>El período de gracia de retención de retención se establece para un dominio de políticas y dicho valor sólo se utiliza cuando ningún otro valor de política está disponible para gestionar una versión de copia de seguridad.</p>
Una clase de gestión específica que debe existir una versión de copia de seguridad para poder migrar un archivo de un nodo de cliente, pero la clase de gestión no contiene ningún valor de copia de seguridad.	Este aviso se aplica únicamente si utiliza el producto IBM Spectrum Protect for Space Management. Los conflictos entre clases de gestión pueden causar problemas a los clientes de IBM Spectrum Protect for Space Management.

Activación de conjunto de políticas

Cuando activa un conjunto de políticas, el servidor valida el contenido del conjunto de políticas y copia el conjunto de políticas para que sea el conjunto de políticas activas. Para modificar posteriormente el contenido del conjunto de políticas activas, debe crear o modificar otro conjunto de políticas y activar dicho conjunto de políticas.

Algunas actualizaciones de políticas tienen un efecto inmediato cuando se activa, pero otras no:

- Las actualizaciones de los valores de Mantener copias de seguridad extra y de Mantener copias de seguridad suprimidas se aplican de forma inmediata a los datos que ya están en el almacenamiento del servidor y a las copias de seguridad futuras.

Si utiliza mandatos, estos valores son los parámetros RETEXTRA y RETONLY para los mandatos DEFINE COPYGROUP o UPDATE COPYGROUP.

- Las actualizaciones de los valores de Copias de seguridad y de Copias de seguridad suprimidas no entran en vigor para los datos del cliente hasta que el cliente completa la siguiente operación de copia de seguridad.

Si utiliza mandatos, estos valores son los parámetros VEREXISTS y VERDELETED para los mandatos DEFINE COPYGROUP o UPDATE COPYGROUP.

Restricciones de los servidores que utilizan la característica de protección de retención de datos

Si la característica de protección de retención de datos se activa, se aplican más reglas al validar y activar un juego de políticas. La característica de protección de retención de datos se activa utilizando el mandato SET ARCHIVERETENTIONPROTECTION en un servidor que no tiene todavía ningún dato de cliente.

Si la protección de retención de datos se activa para un servidor, deben cumplirse varias reglas para que la política se active:

- Si existe una clase de gestión en el conjunto de políticas activas, debe existir una clase de gestión con el mismo nombre en el conjunto de políticas que se va a activar.
- Todas las clases de gestión del conjunto de políticas que se va a activar deben incluir valores de retención de archivado.
- Si el conjunto de políticas incluye valores de retención de archivado en una clase de gestión, el conjunto de políticas que se va a activar debe tener valores de retención de archivado que sean como mínimo tan grandes como los valores correspondientes del conjunto de políticas activas.

Si el servidor es un servidor gestionado en una configuración empresarial, podría recibir actualizaciones desde el servidor que es el gestor de configuración. Las actualizaciones de política recibidas por el servidor gestionado desde el gestor de configuración deben también cumplir las reglas anteriores.

Conceptos relacionados:

[Configuración empresarial \(V7.1.1\)](#)

Referencia relacionada:

SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)

Personalización de una política

Puede personalizar las políticas existentes para que cumplan los requisitos de retención de datos nuevos o revisados de la organización. La modificación de un dominio de políticas o la copia de un dominio de políticas existente es una forma habitual de personalizar una política.

Acerca de esta tarea

Los valores de política de claves están en clases de gestión. En las clases de gestión puede controlar tanto el número de versiones de copia de seguridad como el número de días que se conservarán las versiones de copia de seguridad en el almacenamiento del servidor. Cuando se utilizan ambos tipos de control, la política es más compleja. Si se controla solo el número de días que se conservarán las versiones de copia de seguridad, podrá definir de forma más sencilla durante cuánto tiempo se conservarán los datos de copia de seguridad.

Asegúrese de que la clase de gestión predeterminada de un dominio de políticas tenga los valores adecuados para la retención de datos de la mayor parte de los clientes asignados al dominio. Los valores de retención de la clase de gestión predeterminada se aplican a los datos cuando las operaciones del cliente no especifican una clase de gestión.

Puede trabajar en actualizaciones de una política y guardar los cambios para un momento posterior. Cuando esté satisfecho con los cambios del borrador, puede activar el conjunto de políticas actualizadas para aplicar los cambios.

Procedimiento

1. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
2. Seleccione el dominio de políticas y pulse Aceptar. Pulse Conjuntos de políticas.
3. Pulse el conmutador Configurar para actualizar los valores.
4. Personalice los valores en la clase de gestión.

- a. Realice selecciones para los servicios de copia de seguridad. Por ejemplo, actualice los siguientes elementos para que las versiones de copias de seguridad inactivas de los clientes se conserven durante 30 días:
 - Copias de seguridad: Sin límite
 - Mantener copias de seguridad extra: 30 días
 - Copias de seguridad suprimidas: 1
 - Mantener copias de seguridad suprimidas: Sin límite
 - b. Opcional: Realice selecciones para los servicios de archivado. Por ejemplo, cambie la opción Mantener archivos archivados a 1 año.
 - c. Pulse Guardar.
5. Opcional: Pulse +Clase de gestión para añadir una clase de gestión.
- a. Realice selecciones para los valores básicos y pulse Añadir.
 - b. Personalice más valores en la nueva clase de gestión. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
 - c. Pulse Guardar.
6. En la columna Valor predeterminado, asegúrese de que se ha seleccionado una clase de gestión correcta como predeterminada. Los valores de retención de la clase de gestión predeterminada se aplican cuando las operaciones del cliente no especifican una clase de gestión. Las clases de gestión se pueden especificar al ejecutar una operación de cliente. Una clase de gestión también se puede especificar en un archivo de opciones de cliente que esté en el sistema cliente o en un conjunto de opciones de cliente definido en el servidor.
7. Active el conjunto de políticas pulsando Activar.
8. Asigne nodos cliente al dominio de políticas nuevo actualizando los nodos cliente existentes o inscribiendo nuevos nodos.
- Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
 - Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.
- La retención de datos de cliente que asigne al dominio de políticas ahora se controlará mediante la política.
- Requisito: Si un cliente está en ejecución cuando se asigna a un nuevo dominio, debe detener y reiniciar el cliente para que el cambio surta efecto.

Tareas relacionadas:


Control de las operaciones de cliente mediante conjuntos de opciones de cliente

Creación de una política copiando una política existente

Puede crear nuevas políticas copiando una política existente y, a continuación, actualizando las partes que desea cambiar.

Procedimiento

Puede crear una nueva política copiando un dominio de políticas, actualizando las clases de gestión y, a continuación, asignando clientes al nuevo dominio.

1. En la página Visión general del Centro de operaciones, pase el cursor por encima del icono de valores  y pulse Creador de mandatos.
2. Copie un dominio de políticas utilizando el mandato COPY DOMAIN. Por ejemplo, copie el dominio de políticas predeterminadas, STANDARD, en un nuevo dominio de políticas, NEWDOMAIN:

```
copy domain standard newdomain
```

Esta operación copia el dominio de políticas y todos sus conjuntos de políticas y clases de gestión asociados. En este ejemplo, la operación copia los elementos siguientes en el dominio de políticas NEWDOMAIN:

- Un conjunto de políticas denominado STANDARD.
 - La clase de gestión denominada STANDARD, que se encuentra en el conjunto de políticas STANDARD.
 - Los grupos de copia de la clase de gestión STANDARD contienen:
 - El grupo de copias de seguridad denominado STANDARD
 - El grupo de copias archivadas denominado STANDARD
3. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
 4. Seleccione el dominio de políticas nuevo y pulse Aceptar. Pulse Conjuntos de políticas.
 5. Pulse el conmutador Configurar para actualizar los valores.
 6. Personalice los valores en las clases de gestión.
 - a. Realice selecciones para los servicios de copia de seguridad. Por ejemplo, actualice los siguientes elementos para que las versiones de copias de seguridad inactivas de los clientes se conserven durante 30 días:
 - Copias de seguridad: Sin límite
 - Mantener copias de seguridad extra: 30 días

- Copias de seguridad suprimidas: 1
 - Mantener copias de seguridad suprimidas: Sin límite
 - b. Opcional: Realice selecciones para los servicios de archivado. Por ejemplo, cambie la opción Mantener archivos archivados a 1 año.
 - c. Pulse Guardar.
7. Opcional: Realice otras actualizaciones y adiciones, tales como añadir una clase de gestión.
- a. Pulse +Clase de gestión para añadir una clase de gestión. Realice selecciones para los valores básicos y pulse Añadir.
 - b. Personalice más valores en la nueva clase de gestión. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
 - c. Pulse Guardar.
8. Seleccione la clase de gestión que utilizan los clientes, que se indica en la columna Predeterminada. Pulse Guardar. Los valores de retención de la clase de gestión predeterminada se aplican cuando las operaciones del cliente no especifican una clase de gestión. Las clases de gestión se pueden especificar al ejecutar una operación de cliente. Una clase de gestión también se puede especificar en un archivo de opciones de cliente que esté en el sistema cliente o en un conjunto de opciones de cliente definido en el servidor.
9. Active el conjunto de políticas pulsando Activar.
10. Asigne nodos cliente al dominio de políticas nuevo actualizando los nodos cliente existentes o inscribiendo nuevos nodos.
- Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
 - Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.
- La retención de datos de cliente que asigne al dominio de políticas ahora se controlará mediante la política. Por ejemplo, si ha implementado el ejemplo en el paso 6, las versiones de copia de seguridad inactivas de los clientes se conservan durante 30 días de forma predeterminada.
- Requisito: Si un cliente está en ejecución cuando se asigna a un nuevo dominio, debe detener y reiniciar el cliente para que el cambio surta efecto.

Tareas relacionadas:

Control de las operaciones de cliente mediante conjuntos de opciones de cliente

Creación de un dominio de políticas

Es posible que desee crear un nuevo dominio de políticas para cada tipo de cliente que esté protegido mediante el servidor. Es posible que también desee dividir las responsabilidades de los clientes entre varios administradores concediéndoles autorización para dominios de políticas específicos.


Acerca de esta tarea

La creación de un dominio de políticas puede ser útil en las siguientes circunstancias:

- Las aplicaciones, sistemas o máquinas virtuales necesitan diferentes valores de retención de datos. Puede crear un dominio de políticas para cada tipo de cliente, con una política predeterminada que sea adecuada para ese tipo.
- Los administradores son responsables de distintos grupos de clientes. Para cada administrador, puede crear un dominio de políticas al que asignará los clientes que va a gestionar ese administrador.

Procedimiento

Los pasos siguientes resumen cómo crear un dominio de políticas.

1. En la página Visión general del Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.
2. Defina un dominio de políticas utilizando el mandato DEFINE DOMAIN.
3. Defina un conjunto de políticas para el dominio utilizando el mandato DEFINE POLICYSET.
4. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
5. Seleccione el dominio de políticas y pulse Aceptar. Pulse Conjuntos de políticas.
6. Pulse el conmutador Configurar para actualizar los valores.
7. Pulse +Clase de gestión para añadir una clase de gestión. Realice selecciones para los valores básicos y pulse Añadir.
8. Opcional: Personalice más valores en la nueva clase de gestión:
 - a. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas.
 - b. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
 - c. Pulse Guardar.
9. Opcional: Pulse +Clase de gestión para añadir más clases de gestión.

10. En la columna Valor predeterminado, asegúrese de que se ha seleccionado una clase de gestión predeterminada.
11. Active el conjunto de políticas pulsando Activar.
12. Asigne clientes al nuevo dominio de políticas. En la barra de menús del Centro de operaciones, haga clic en Clientes.
 - o Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
 - o Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.

Referencia relacionada:

DEFINE DOMAIN (Definir un nuevo dominio de políticas)

DEFINE POLICYSET (Definir un juego de políticas)

Control de las operaciones de cliente mediante conjuntos de opciones de cliente

Puede utilizar conjuntos de opciones de cliente para controlar de forma centralizada las opciones de proceso que utilizan los clientes para operaciones, tales como una copia de seguridad. Los conjuntos de opciones de cliente garantizan que los datos estén protegidos de forma coherente de acuerdo con sus requisitos. Un conjunto de opciones de cliente pueden reemplazar las opciones en un archivo de opciones de cliente y añadir opciones que podrían no estar en un archivo de opciones del cliente local.

Acerca de esta tarea

Al crear y asignar conjuntos de opciones de cliente, reduce la necesidad de actualizar archivos de opciones de cliente local y la cantidad de trabajo que deben realizar los usuarios.

Por ejemplo, puede definir un conjunto de opciones de cliente para especificar una lista de inclusión/exclusión que determina qué se incluirá o excluirá de la copia de seguridad y qué clases de gestión se utilizarán para gestionar retenciones de datos. Otras opciones que pueden ser útiles para el control de forma centralizada en un conjunto de opciones de cliente son compression y deduplication.

Puede crear conjuntos de opciones de cliente para clientes que tengan unas necesidades similares, como clientes en el mismo sistema operativo, clientes que utilizan el mismo software o clientes que utiliza un departamento. Por ejemplo, puede crear conjuntos de opciones de cliente para estaciones de trabajo Windows o para el departamento de nóminas. Después de crear el conjunto de opciones de cliente, asigne el conjunto a todos los clientes del mismo tipo.

No todas las opciones de cliente se pueden especificar en un conjunto de opciones de cliente en el servidor. Para obtener información acerca de las opciones de cliente que puede controlar centralmente en un conjunto de opciones de cliente, consulte Las opciones de cliente las puede establecer el servidor.

Procedimiento

1. Defina un conjunto de opciones de cliente utilizando el mandato DEFINE CLOPTSET. Por ejemplo, para definir un conjunto de opciones de cliente con el nombre PAYROLLBACKUP, emita el mandato siguiente:

```
define cloptset payrollbackup description='Opciones de copia de seguridad para el departamento de nóminas'
```

2. Añada opciones de cliente al conjunto de opciones de cliente utilizando el mandato DEFINE CLIENTOPT. Por ejemplo, desea añadir las opciones include y exclude al conjunto de opciones de cliente denominado PAYROLLBACKUP para lograr los objetivos siguientes:

- o Excluir archivos de directorio temporales de internet de las operaciones de copia de seguridad
- o Incluir en la copia de seguridad todos los archivos del directorio C:\Data y sus subdirectorios y asignar los archivos a la clase de gestión PAYCLASS para retención de datos

Emita los siguientes mandatos:

```
define clientopt payrollbackup inclexcl "exclude.dir '*:\...\Archivos temporales de internet'"  
define clientopt payrollbackup inclexcl "include C:\Data\...\* payclass"
```

3. Para asignar un conjunto de opciones de cliente a un cliente, siga los pasos siguientes:
 - a. En la página Visión general de Centro de operaciones, pulse Clientes.
 - b. Seleccione un cliente y pulse Detalles.
 - c. Pulse Propiedades.
 - d. En el área General, seleccione un conjunto de opciones y pulse Guardar.

Referencia relacionada:

DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)

DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)

- ☞ Opción de cliente de compresión
- ☞ Opción de cliente de eliminación de duplicados

Configuración del almacenamiento

En función de la funcionalidad de almacenamiento que necesite, elija el tipo correcto de soporte de almacenamiento. Optimice y controle sus agrupaciones de almacenamiento para distintos tipos de datos.

- **Tipos de agrupaciones de almacenamiento**
Para ayudarle a determinar qué tipo de agrupación de almacenamiento satisface mejor sus requisitos de almacenamiento, debe evaluar las características de cada tipo de agrupación de almacenamiento.
- **Opciones de eliminación de datos duplicados**
Utilice la eliminación de duplicados de datos en línea para eliminar las duplicaciones y escribir los datos en una agrupación de almacenamiento de contenedores al mismo tiempo. Utilice la eliminación de datos duplicados postproceso para eliminar datos duplicados de las agrupaciones de almacenamiento de acceso secuencial (FILE) .
- **Configuración de dispositivos de almacenamiento**
Configure dispositivos de almacenamiento conectando dispositivos, configurando controladores de dispositivo y creando los objetos que representan los dispositivos para el servidor.
- **Configuración de una agrupación de almacenamiento de contenedores de directorios para almacenamiento de datos**
Puede configurar las agrupaciones de almacenamiento de contenedores de directorios para utilizar la deduplicación de datos en línea y almacenar los datos deduplicados.
- **Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos**
Puede almacenar datos duplicados y sin duplicar en una agrupación de almacenamiento de contenedores en la nube y restaurar los datos cuando lo necesite. Puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar uno de los siguientes protocolos y proveedores de servicios: Amazon Web Services (AWS) con Simple Storage Service (S3), IBM® Cloud Object Storage con Swift o S3 (e IBM SoftLayer), Microsoft Azure, y OpenStack con Swift utilizando Keystone versión 1 o versión 2. Las agrupaciones de almacenamiento de contenedores en la nube no se admiten en Linux on System z.
- **Definición de una regla de almacenamiento para los niveles en la nube**
Puede definir una regla de almacenamiento para implementar los niveles en la nube, que mueven los datos de una agrupación de almacenamiento de contenedores de directorios en disco a una agrupación de almacenamiento de contenedores en la nube. La regla de almacenamiento planifica los niveles en la nube desde las agrupaciones de almacenamiento de contenedor del directorio a las agrupaciones de almacenamiento del contenedor en la nube.
- **Optimización de rendimiento para almacenamiento de objetos en la nube**
Puede configurar IBM Spectrum Protect para almacenar datos temporalmente en uno o más directorios de agrupación de almacenamiento local durante la ingestión de datos. Los datos se han movido desde el almacenamiento local a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado.
- **Gestión del espacio en las agrupaciones de almacenamiento de contenedor**
Después de configurar IBM Spectrum Protect y añadir almacenamiento, gestione los datos y el espacio de la agrupación de almacenamiento de forma eficaz para asegurarse de que funcione correctamente. Utilice agrupaciones de almacenamiento de contenedores para maximizar el espacio de almacenamiento y el rendimiento del servidor.
- **Auditoría de un contenedor de la agrupación de almacenamiento**
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre la información de base de datos y un contenedor de una agrupación de almacenamiento.
- **Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos**
Puede utilizar muchos tipos de almacenamiento para el servidor IBM Spectrum Protect. Si utiliza almacenamiento de disco de bloque, unidades de estado sólido (SSD) o sistemas de archivos conectados a red para el almacenamiento de servidor, asegúrese de que el almacenamiento cumple los requisitos.

Tipos de agrupaciones de almacenamiento

Para ayudarle a determinar qué tipo de agrupación de almacenamiento satisface mejor sus requisitos de almacenamiento, debe evaluar las características de cada tipo de agrupación de almacenamiento.

Utilice la tabla siguiente para evaluar cada tipo de agrupación de almacenamiento.

Tipo de agrupación de almacenamiento	Descripción	Usos
--------------------------------------	-------------	------

Tipo de agrupación de almacenamiento	Descripción	Usos
Agrupación de almacenamiento de contenedores de directorios	Una agrupación de almacenamiento primaria que utiliza un servidor para almacenar datos. Los datos que se almacenan en las agrupaciones de almacenamiento de contenedores de directorios utilizan la eliminación de duplicados de datos en línea o la del lado del cliente. Puede utilizar los niveles de nube para mover los datos de las agrupaciones de almacenamiento del contenedor del directorio a las agrupaciones de almacenamiento del contenedor en la nube.	<p>Utilícelo cuando desee eliminar los duplicados de datos en línea. Al utilizar agrupaciones de almacenamiento de contenedores de directorio, elimina la necesidad de reclamación de volumen, lo que mejora el rendimiento de servidor y reduce el coste del hardware de almacenamiento.</p> <p>No puede utilizar este tipo de agrupación de almacenamiento para operaciones de copia de seguridad, migración, reclamación, importación o exportación de agrupaciones de almacenamiento.</p>
Agrupación de almacenamiento de contenedores en la nube	Una agrupación de almacenamiento primaria que utiliza un servidor para almacenar datos. Utilice las agrupaciones de almacenamiento de contenedores en la nube para almacenar los datos en un proveedor de almacenamiento en la nube basado en almacenamiento de objetos. Los datos que se almacenan en agrupaciones de almacenamiento del contenedor en la nube utilizan o bien la deduplicación de datos en línea o bien la deduplicación de datos del lado del cliente.	<p>Mediante el almacenamiento de datos en agrupaciones de almacenamiento de contenedores en la nube, puede aprovechar las ventajas de coste por unidad que ofrecen las nubes junto con las prestaciones de escalabilidad que proporciona el almacenamiento en nube.</p> <p>No puede utilizar este tipo de agrupación de almacenamiento para operaciones de copia de seguridad, migración, reclamación, importación o exportación de agrupaciones de almacenamiento.</p>
Agrupación de almacenamiento de acceso aleatorio	Un conjunto de volúmenes que el servidor utiliza para almacenar las versiones de copia de seguridad de archivos, los archivos que son copias archivadas y los archivos migrados. Los archivos se almacenan en dispositivos de disco, DISK.	<p>Utilice este tipo de agrupación de almacenamiento para mantener una copia de los datos en dispositivos de DISCO. Puede migrar datos a estas agrupaciones de almacenamiento o fuera desde las mismas desde los siguientes tipos de agrupaciones de almacenamiento:</p> <ul style="list-style-type: none"> • Agrupaciones de almacenamiento de acceso aleatorio • Agrupaciones de almacenamiento de acceso secuencial
Agrupación de almacenamiento de acceso secuencial	Un conjunto de volúmenes que el servidor utiliza para almacenar las versiones de copia de seguridad de archivos, los archivos que son copias archivadas y los archivos migrados desde nodos cliente. Los archivos se almacenan en cinta o en dispositivos FILE. Los datos que se almacenan en las agrupaciones de almacenamiento de contenedores de acceso secuencial utilizan la eliminación de duplicados de datos de postproceso y del lado del cliente. Restricción: La deduplicación de datos de postproceso solo está disponible en la versión 7.1.2 y en versiones anteriores a esta.	<p>Utilice este tipo de agrupación de almacenamiento para mantener una copia de los datos en dispositivos de ARCHIVO y de CINTA. Puede migrar datos a este tipo de agrupación de almacenamiento.</p>

Tipo de agrupación de almacenamiento	Descripción	Usos
Agrupación de almacenamiento de copia	Conjunto de volúmenes que contiene copias de archivos que residen en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copias se utilizan solo para realizar copias de seguridad de datos que están almacenados en agrupaciones de almacenamiento primarias. Una agrupación de almacenamiento de copia no puede ser el destino de un grupo de copia de seguridad, de un grupo de copia archivada ni de una clase de gestión (para archivos bajo gestión de espacio).	<p>Utilice las agrupaciones de almacenamiento de copia para tener una copia de datos activos e inactivos que puede restaurar en una agrupación de almacenamiento primaria después de un desastre o de una parada.</p> <p>No puede utilizar la eliminación de duplicados de datos en línea, la compresión, la réplica o la eliminación de duplicados de datos con este tipo de agrupación de almacenamiento.</p>
Agrupación de almacenamiento de copia de contenedor	Un conjunto de volúmenes de cinta que contiene una copia de las extensiones con eliminación de duplicados que residen en una agrupación de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor se utilizan solo para proteger los datos almacenados en las agrupaciones de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor se utilizan para reparar los daños en una agrupación de almacenamiento de contenedores de directorio o para restaurar una agrupación de almacenamiento de contenedores de directorios si se produce un siniestro. Las agrupaciones de almacenamiento de copia de contenedor se almacenan en soporte secuencial.	<p>Utilice las agrupaciones de almacenamiento de copia de contenedor para almacenar copias de agrupaciones de directorios en el local o fuera del local. Los datos dañados en las agrupaciones de directorios se pueden reparar utilizando las extensiones deduplicadas de una agrupación de almacenamiento de copia de contenedor.</p>
Agrupación de almacenamiento de datos activos	Conjunto de volúmenes de agrupación de almacenamiento que contiene sólo versiones activas de datos de copia de seguridad de cliente.	<p>Utilice agrupaciones de almacenamiento de datos activos para restaurar únicamente los datos activos en agrupaciones de almacenamiento primario después de un desastre o una parada. Cuando se restauran datos activos, puede restaurar datos de cliente más rápidamente, a la vez que utiliza menos ancho de banda.</p> <p>No puede utilizar la eliminación de duplicados de datos en línea, la compresión, la réplica o la eliminación de duplicados de datos con este tipo de agrupación de almacenamiento.</p>

Utilice la tabla siguiente para comparar las posibilidades de las agrupaciones de almacenamiento y elegir la agrupación de almacenamiento que mejor se ajuste a sus necesidades de negocio en función de los requisitos de almacenamiento.

Objetivo del usuario	Agrupación de almacenamiento de contenedores de directorios	Agrupación de almacenamiento de contenedores en la nube	Agrupación de almacenamiento de acceso aleatorio	Agrupación de almacenamiento de acceso secuencial	Agrupación de almacenamiento de copia	Agrupación de almacenamiento de copia de contenedor	Agrupación de almacenamiento de datos activos

Objetivo del usuario	Agrupación de almacenamiento de contenedores de directorios	Agrupación de almacenamiento de contenedores en la nube	Agrupación de almacenamiento de acceso aleatorio	Agrupación de almacenamiento de acceso secuencial	Agrupación de almacenamiento de copia	Agrupación de almacenamiento de copia de contenedor	Agrupación de almacenamiento de datos activos
Proteja los datos de la agrupación de almacenamiento mediante la réplica de nodos.	✓		✓	✓	✓		✓
Reduzca las necesidades de almacenamiento mediante la compresión en línea.	✓	✓					
Reduzca las necesidades de almacenamiento utilizando la eliminación de duplicados de datos en línea.	✓	✓					
Reduzca las necesidades de almacenamiento utilizando la eliminación de duplicados de datos del lado del cliente.	✓	✓		✓			
Reduzca las necesidades de almacenamiento utilizando la eliminación de duplicados de datos de postproceso.				✓			
Proteja los datos de la agrupación de almacenamiento mediante la protección de agrupaciones de almacenamiento.	✓					✓	

Objetivo del usuario	Agrupación de almacenamiento de contenedores de directorios	Agrupación de almacenamiento de contenedores en la nube	Agrupación de almacenamiento de acceso aleatorio	Agrupación de almacenamiento de acceso secuencial	Agrupación de almacenamiento de copia	Agrupación de almacenamiento de copia de contenedor	Agrupación de almacenamiento de datos activos
Realice una copia de seguridad de los datos de la agrupación de almacenamiento utilizando las agrupaciones de almacenamiento de copia en disco o cinta.			✓	✓			
Almacene datos en la nube.		✓					
Utilice los niveles en la nube para mover datos de una agrupación de almacenamiento del contenedor de directorios a una agrupación de almacenamiento del contenedor en la nube.	✓						

Opciones de eliminación de datos duplicados

Utilice la eliminación de duplicados de datos en línea para eliminar las duplicaciones y escribir los datos en una agrupación de almacenamiento de contenedores al mismo tiempo. Utilice la eliminación de datos duplicados postproceso para eliminar datos duplicados de las agrupaciones de almacenamiento de acceso secuencial (FILE) .

Debe utilizar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de contenedores en la nube para la eliminación de duplicados de datos en línea. Si utiliza agrupaciones de almacenamiento de contenedores de directorio o de contenedor en la nube, reducirá la necesidad de realizar una reorganización fuera de línea y, de esta forma, se mejorará el rendimiento de servidor y se reducirá el coste del hardware de almacenamiento. No utilice clases de dispositivo o volúmenes con estos tipos de agrupación de almacenamiento.

Mediante la eliminación de datos duplicados postproceso, el servidor identifica en primer lugar los datos y después elimina los datos duplicados de la agrupación de almacenamiento. En el soporte de almacenamiento solo se conserva una instancia de los datos. Otras instancias de los mismos datos se sustituyen por un puntero a la instancia retenida. Cuando elimine datos duplicados, podrá reclamar espacio en la agrupación de almacenamiento.

Para obtener más información sobre la eliminación de datos duplicados postproceso, consulte el Eliminación de datos duplicados (V7.1.1).

En la eliminación de datos duplicados del lado del cliente, solo se envían al servidor datos deduplicados y comprimidos. El proceso se distribuye entre el servidor y el cliente durante un proceso de copia de seguridad.

Utilice la tabla siguiente para comparar opciones de deduplicación de datos.

Tipo de deduplicación de datos	Ventajas	Inconvenientes
Postproceso Restricción: Puede utilizar la deduplicación de datos postproceso para eliminar solo las agrupaciones de almacenamiento de acceso secuencial (FILE).	<ul style="list-style-type: none"> Tras la deduplicación de datos, puede reclamar la agrupación de almacenamiento. 	<ul style="list-style-type: none"> Tiempos de proceso más largos, porque los datos se deben identificar para poder eliminar los datos duplicados de la agrupación de almacenamiento.
En línea Restricción: Solo puede utilizar la deduplicación de datos en línea con las agrupaciones de almacenamiento de contenedores de directorio y de contenedores en la nube.	<ul style="list-style-type: none"> Deduplica los datos a medida que se escriben en una agrupación de almacenamiento de contenedores. Reduce la necesidad de reorganización fuera de línea, lo que mejora el rendimiento del servidor. Menor coste del hardware de almacenamiento. 	<ul style="list-style-type: none"> Mayor grado de utilización de procesador por parte del servidor.
En el lado del cliente	<ul style="list-style-type: none"> El proceso se distribuye entre el servidor y el cliente durante un proceso de copia de seguridad. 	<ul style="list-style-type: none"> Mayor grado de utilización de procesador por parte del cliente. Las operaciones del cliente tales como copias de seguridad tardan más tiempo en efectuarse. Sólo los datos comprimidos y deduplicados se envían al servidor.

Tareas relacionadas:




- Configuración de eliminación de duplicados de datos (solución de disco multisitio)
- Configuración de eliminación de duplicados de datos (solución de disco de un solo sitio)
- Comparación de agrupaciones de almacenamiento

Configuración de dispositivos de almacenamiento

Configure dispositivos de almacenamiento conectando dispositivos, configurando controladores de dispositivo y creando los objetos que representan los dispositivos para el servidor.

Acerca de esta tarea

Si no va a utilizar la solución de disco de sitio único o de sitio múltiple, configure y gestione dispositivos de almacenamiento siguiendo las instrucciones de la documentación relativa a la V7.1.1:

-  Sistemas operativos AIX  Sistemas operativos Linux Configuración y gestión de los dispositivos de almacenamiento
-  Sistemas operativos Windows Configuración y gestión de los dispositivos de almacenamiento

Configuración de una agrupación de almacenamiento de contenedores de directorios para almacenamiento de datos

Puede configurar las agrupaciones de almacenamiento de contenedores de directorios para utilizar la deduplicación de datos en línea y almacenar los datos deduplicados.

Procedimiento


Para almacenar datos en una agrupación de almacenamiento de contenedores de directorios, complete los pasos siguientes:

- Para crear una agrupación de almacenamiento de contenedores de directorios, siga estos pasos:
 - En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
 - En la página Agrupaciones de almacenamiento, pulse + Agrupación de almacenamiento.
 - Realice los pasos del asistente Añadir agrupación de almacenamiento. Seleccione Directorio como tipo de almacenamiento basado en contenedor.
- Cuando el asistente haya creado la agrupación de almacenamiento, actualice las clases de gestión y los conjuntos de políticas para que se utilice la nueva agrupación. Para actualizar una clase de gestión para utilizar la nueva agrupación, complete los pasos siguientes:
 - En la barra de menús de Centro de operaciones, pulse Servicios.

- b. En la página Políticas, seleccione un dominio de políticas y pulse Detalles.
 - c. En la página Detalles, pulse la pestaña Conjunto de políticas.
 - d. Pulse el conmutador Configurar. Los conjuntos de políticas se pueden editar.
 - e. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
 - f. Actualice una o más clases de gestión para utilizar la nueva agrupación editando el campo Destino de copia de seguridad de la tabla.
 - g. Pulse Guardar.
3. Active el conjunto de políticas cambiado completando los pasos siguientes:
 - a. Pulse Activar. Como cambiar el conjunto de políticas activo puede provocar la pérdida de datos, se muestra un resumen de las diferencias entre el conjunto de políticas activo y el nuevo conjunto de políticas.
 - b. Mire las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a las clases de gestión del conjunto de políticas actualmente activo se enlazan, después de la activación, a las clases de gestión con los mismos nombres del nuevo conjunto de políticas.
 - c. Identifique las clases de gestión del conjunto de políticas actualmente activo que no tiene contrapartidas en el nuevo conjunto de políticas, y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión los gestiona, después de la activación, la clase de gestión predeterminada en el nuevo conjunto de políticas.
 - d. Si los cambios implementados por el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.
 4. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

Qué hacer a continuación

Para proteger una agrupación de almacenamiento de contenedores de directorio, utilice el mandato PROTECT STGPOOL. Para obtener las instrucciones, consulte la sección PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento) y la sección Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta.

 Sistemas operativos Linux Si está protegiendo una agrupación de almacenamiento de contenedores de directorios copiando los datos en un servidor remoto y tiene problemas de red, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

- Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta
Puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios copiando los datos a agrupaciones de almacenamiento de copia de contenedor, que se representan mediante volúmenes de cinta. La copia de cinta se utiliza para reparar daños en una agrupación de almacenamiento de contenedores de directorios.
- Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado
Si su solución de almacenamiento incluye agrupaciones de almacenamiento de copias de contenedores que se representan por medio de volúmenes de cinta, pero no ha configurado la función del gestor de recuperación tras desastre (DRM), puede seguir un procedimiento manual para rotar los volúmenes de cinta fuera del local. Al mantener copias de los datos en volúmenes de cinta fuera del local, puede restaurar los datos si se produce un siniestro en el local.
- Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor
De forma predeterminada, la reclamación de volumen de cinta está habilitada para las agrupaciones de almacenamiento de copia de contenedor. Para asegurarse de que los volúmenes de cinta se utilizan de forma eficaz, puede cambiar el umbral para la reclamación de volumen.
- Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor
Puede reclamar los volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor sin ejecutar ninguna operación de protección cuando no tenga tiempo para permitir operaciones de protección y reclamación.
- Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro
Determine si las agrupaciones de almacenamiento de copia de contenedor cumplen los requisitos de protección frente a siniestro.

Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta

Puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios copiando los datos a agrupaciones de almacenamiento de copia de contenedor, que se representan mediante volúmenes de cinta. La copia de cinta se utiliza para reparar daños en una agrupación de almacenamiento de contenedores de directorios.

Antes de empezar

Defina como mínimo una biblioteca de cintas en el servidor con el mandato DEFINE LIBRARY. Suministre suficientes unidades de cintas y volúmenes reutilizables para satisfacer los requisitos de almacenamiento. Para obtener más información sobre cómo gestionar los soportes de copia de seguridad y configurar el gestor de recuperación ante siniestro (DRM), consulte Gestor de recuperación ante siniestro (V7.1.1).

Acerca de esta tarea

Para copiar los datos de las agrupaciones de almacenamiento de contenedores de directorio en cinta, el Centro de operaciones crea una planificación para ejecutar el mandato PROTECT STGPOOL. Cuando se ejecuta la planificación de protección, se crea una copia de cinta. Al menos debe estar disponible un volumen cuando se ejecuta la planificación de protección. De lo contrario, la operación no será satisfactoria.

Puede crear hasta dos copias de cinta, pero debe utilizar la interfaz de línea de mandatos para crear una segunda agrupación de almacenamiento de copia de contenedor. Una copia de cinta se puede llevar a una ubicación de recuperación ante siniestro fuera del local. La otra copia puede conservarse en el local para facilitar la recuperación de anomalías menos críticas.

Restricciones:

- Las bibliotecas de cintas virtuales no están soportadas, independientemente del tipo de biblioteca que se defina. Solo recibe soporte la cinta física.
- Las agrupaciones de almacenamiento de copia de contenedor se pueden utilizar para reparar daños menos a moderados de la agrupación de almacenamiento, lo que incluye contenedores o directorios dañados. Las agrupaciones de almacenamiento de copia de contenedor también se pueden utilizar para la protección frente a siniestro, pero debe asegurarse de que los tiempos de recuperación cumplan sus requisitos. Para obtener más información, consulte Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro.
- No puede utilizar la réplica para dirigirse a una agrupación de almacenamiento de copia de contenedor.
Consejo: Puede crear una copia de cinta de los datos de agrupación de almacenamiento de contenedores del directorio en un sitio de recuperación tras desastre mediante un procedimiento para crear una agrupación de almacenamiento de copia de contenedor en el servidor de réplica de destino. Después, programe los mandatos PROTECT STGPOOL y REPLICATE NODE para ejecutarlo en el servidor de réplica fuente para proteger sus datos en el servidor de réplica de destino.
- No puede utilizar el procedimiento siguiente si la agrupación de almacenamiento de contenedores de directorios ya tiene una agrupación de almacenamiento de copia de contenedor asociada. Para crear una segunda agrupación de almacenamiento de copia de contenedor, siga las instrucciones del paso 5.

Si ha creado una agrupación de almacenamiento de copia de contenedor como parte del asistente Añadir agrupación de almacenamiento, no es necesario que utilice este procedimiento. Cuando haya completado el asistente, el Centro de operaciones habrá configurado la agrupación de almacenamiento de copia de contenedor y una planificación de protección.

Procedimiento

Para configurar la protección de la agrupación de almacenamiento para una agrupación de almacenamiento de contenedores de directorio, siga estos pasos:

1. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
2. En la página Agrupaciones de almacenamiento, seleccione la agrupación de almacenamiento de contenedores de directorio que desea proteger en cinta.
3. Pulse Más > Añadir agrupación de copia de contenedor.
4. Siga las instrucciones de la ventana Añadir agrupación de copia de contenedor para planificar la protección en cinta.
5. Después de completar los pasos anteriores, puede añadir una segunda agrupación de almacenamiento de copia de contenedor utilizando la interfaz de línea de mandatos. Opcionalmente, siga los pasos siguientes para añadir una agrupación de almacenamiento de copia de contenedor:
 - a. Cree una agrupación de almacenamiento de copia de contenedor emitiendo el mandato DEFINE STGPOOL.
 - b. Asigne la agrupación de almacenamiento de copia de contenedor a la agrupación de almacenamiento de contenedores de directorio emitiendo el mandato UPDATE STGPOOL para la agrupación de contenedor de directorio.

Resultados

Después de completar la configuración, los datos de la agrupación de almacenamiento de contenedores de directorios se copiará a una agrupación de almacenamiento de copia de contenedor basada en la planificación de protección definida.

Qué hacer a continuación

1. Si ha creado una copia de cinta para el almacenaje externo, habilite la agrupación de almacenamiento externa de copia de contenedor para operaciones DRM emitiendo el mandato SET DRMCOPYCONTAINERSTGPOOL. Asegúrese de que los volúmenes de cinta se añadan a las planificaciones de rotación de cintas externas. Si no se ha configurado DRM, deberá hacerlo o utilizar un

método alternativo para rotar las cintas fuera del local. Para obtener instrucciones sobre el método alternativo, consulte Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado. Para verificar que las agrupaciones de copia de contenedor fuera del local están habilitadas para DRM, utilice el mandato QUERY DRMSTATUS.

Para obtener las instrucciones acerca de cómo configurar DRM, consulte Disaster Recovery Manager (V7.1.1).

2. Confirme que el umbral de reclamación para la agrupación de almacenamiento de copia de contenedor cumpla con sus requisitos.

De forma predeterminada, la reclamación de volumen de cinta está habilitada para nuevas agrupaciones de almacenamiento de copia de contenedor que se crean utilizando el Centro de operaciones. La reclamación de volúmenes se lleva a cabo cuando el umbral de reclamación de la agrupación de almacenamiento de copia de contenedor está por debajo del 100%. Sin embargo, los volúmenes de cinta no son candidatos para la reclamación hasta que están llenos en un 75%. Tenga cuidado cuando utilice la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para la reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Para evitar que se sobrescriban los volúmenes inmediatamente después de que hayan sido suprimidas todas las extensiones, utilice el parámetro REUSEDELAY para especificar un valor mayor que 0. El Centro de operaciones establece el umbral de reclamación en 60 % para las agrupaciones de almacenamiento de copia de contenedor locales.

Para obtener instrucciones sobre cómo cambiar el umbral de reclamación, consulte Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor.

3. Proteja los metadatos para la agrupación de almacenamiento de copia de contenedor.

Cuando se ejecute la planificación de protección, las extensiones de datos de las agrupaciones de almacenamiento de copia de contenedor se copian en los volúmenes de cinta sin los metadatos asociados. Estos metadatos son necesarios para restaurar las copias de cinta. Para proteger los metadatos, debe realizar por separador la copia de seguridad de la base de datos del servidor, junto con su historial de volúmenes, las opciones de servidor y los archivos de configuración de los dispositivos. Si utiliza la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes de cinta fuera del local, asegúrese de que se cumplan los requisitos siguientes para proporcionar la protección de recuperación ante siniestro:

- Las operaciones de copia de seguridad de base de datos se ejecutan después de que estén finalizadas las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM.
- Todos los volúmenes de copia de seguridad de base de datos y los volúmenes de DRM se trasladan fuera del local conjuntamente.

Para obtener las instrucciones acerca de cómo realizar la copia de seguridad de la base de datos del servidor y los archivos relacionados, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

4. Opcionalmente, cambie la planificación de protección para una agrupación de almacenamiento de contenedores de directorios que tiene una o más agrupaciones de almacenamiento de copia de contenedor asociadas utilizando el mandato UPDATE SCHEDULE. La planificación creada por el Centro de operaciones se denomina CONTAINER_COPY.

Conceptos relacionados:

Almacenamiento de datos en agrupaciones de almacenamiento de copia de contenedor

Tareas relacionadas:

Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

Referencia relacionada:

DEFINE LIBRARY (Definir una biblioteca)

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

UPDATE SCHEDULE (Actualizar una planificación de administración)

QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)

Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado

Si su solución de almacenamiento incluye agrupaciones de almacenamiento de copias de contenedores que se representan por medio de volúmenes de cinta, pero no ha configurado la función del gestor de recuperación tras desastre (DRM), puede seguir un procedimiento manual para rotar los volúmenes de cinta fuera del local. Al mantener copias de los datos en volúmenes de cinta fuera del local, puede restaurar los datos si se produce un siniestro en el local.

Procedimiento

1. Compruebe el volumen de almacenamiento que debe rotarse fuera del local utilizando el mandato CHECKOUT LIBVOLUME.

2. Actualice el volumen para indicar que se mueve fuera del local utilizando el mandato UPDATE VOLUME y especificando ACCESS=UNAVAILABLE. Opcionalmente, indique la ubicación fuera del local utilizando el parámetro LOCATION. Por ejemplo, especifique LOCATION=SITE1.
3. Reclame espacio realizando una de las siguientes acciones:
 - o Para reclamar espacio sin proteger la agrupación de almacenamiento, ejecute el mandato PROTECT STGPOOL y especifique TYPE=LOCAL y RECLAIM=ONLY.
 - o Para reclamar espacio protegiendo la agrupación de almacenamiento, ejecute el mandato PROTECT STGPOOL sin especificar RECLAIM=ONLY.
4. Supervise el volumen utilizando el mandato QUERY VOLUME. Si el volumen se muestra no disponibles y vacío, devuelva el volumen en el sitio e incorpórelo a la biblioteca utilizando el mandato CHECKIN LIBVOLUME.
5. Actualice el mandato utilizando el mandato UPDATE VOLUME y especificando ACCESS=READWRITE.

Referencia relacionada:

CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor

De forma predeterminada, la reclamación de volumen de cinta está habilitada para las agrupaciones de almacenamiento de copia de contenedor. Para asegurarse de que los volúmenes de cinta se utilizan de forma eficaz, puede cambiar el umbral para la reclamación de volumen.

Procedimiento

1. En la página Centro de operaciones Visión general, pulse Almacenamiento > Agrupaciones de almacenamiento.
2. Seleccione la agrupación de almacenamiento y pulse Detalles y, a continuación, Propiedades.
3. En la sección Reclamación, establezca el porcentaje de reclamación y pulse Guardar.
Consejo: De forma alternativa, cambie el umbral de reclamación emitiendo el mandato UPDATE STGPOOL con el parámetro RECLAIM. Para obtener más detalles sobre el parámetro RECLAIM, consulte los mandatos para definir y actualizar las agrupaciones de almacenamiento de copia de contenedor.
Restricción: No puede utilizar el mandato RECLAIM STGPOOL para reclamar volúmenes en las agrupaciones de almacenamiento de copia de contenedor. Para obtener detalles sobre cómo reclamar volúmenes en las agrupaciones de almacenamiento de copia de contenedor, consulte el parámetro RECLAIM en el mandato PROTECT STGPOOL.

Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor

Puede reclamar los volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor sin ejecutar ninguna operación de protección cuando no tenga tiempo para permitir operaciones de protección y reclamación.

Acerca de esta tarea

Cuando emite el mandato PROTECT STGPOOL y la agrupación de almacenamiento de destino es una agrupación de almacenamiento de contenedor, las operaciones de protección y reclamación se ejecutan de forma predeterminada. La práctica preferida es permitir las operaciones de protección y reclamación que se desean ejecutar. Sin embargo, para ahorrar tiempo puede ejecutar únicamente la operación de protección de agrupación de almacenamiento o sólo reclamación, o puede limitar el número de volúmenes de cinta que están reclamados. Utilice este procedimiento sólo cuando tenga que reclamar volúmenes de cinta rápidamente tiempo o cuando tenga que reclamar un número limitado de volúmenes de cinta.

Procedimiento

Para reclamar volúmenes de cinta que ejecutan la operación de protección de agrupación de almacenamiento, realice los pasos siguientes:

1. Opcional: Para maximizar la cantidad de espacio que se reclama, inicie el proceso de caducidad de inventario con el mandato EXPIRE INVENTORY.
2. Determine si desea que la reclamación se ejecute hasta su finalización o si desea limitar el número de volúmenes de cinta reclamados.

3. Para ejecutar la reclamación hasta su finalización, emite el mandato PROTECT STGPOOL y especifique los parámetros TYPE=LOCAL y RECLAIM=ONLY. Por ejemplo, para reclamar espacio en una agrupación de almacenamiento de copia de contenedor local que esté definido como protección de destino para SPOOL1, emita el mandato siguiente:

```
protect stgpool spool1 type=local reclaim=only
```

4. Para reclamar un número limitado de volúmenes, realice los pasos siguientes:

- a. Defina un límite de reclamaciones para la agrupación de almacenamiento de copia de contenedor emitiendo el mandato UPDATE STGPOOL y especificando el parámetro RECLAIMLIMIT. Este parámetro limita al número de volúmenes de la agrupación de almacenamiento de copia de contenedor reclamados.
- b. Emita el mandato PROTECT STGPOOL y especifique el parámetro TYPE=LOCAL con el parámetro RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED.

Consejo: Si especifica RECLAIM=YESLIMITED, las operaciones de reclamación y de protección de la agrupación de almacenamiento se ejecutan cuando se emite el mandato PROTECT STGPOOL. Si especifica RECLAIM=ONLYLIMITED, la reclamación es la única operación que se ejecuta. Si especifica cualquiera de estos valores, la reclamación sólo se ejecuta hasta que alcanza el límite de reclamaciones definido para la agrupación de almacenamiento de copia de contenedores. El límite de reclamación se define con el parámetro RECLAIMLIMIT en el mandato DEFINE STGPOOL o UPDATE STGPOOL.

Por ejemplo, reclamar un límite para cinco volúmenes de cinta en una agrupación de almacenamiento de copia de contenedor que se llama CCPOOL1 sin ejecutar una operación de protección en la agrupación de almacenamiento de contenedores del directorio de origen que recibe el nombre de SPOOL1, emita los siguientes mandatos:

```
actualizar stgpool ccpool1 reclaimlimit=5  
protect stgpool spool1 type=local reclaim=onlylimited
```

For example, para proteger una agrupación de almacenamiento con el nombre SPOOL1 y reclamar un máximo de 10 volúmenes de cinta en la agrupación de almacenamiento, emita los siguientes mandatos:

```
update stgpool spool1 reclaimlimit=10  
protect stgpool spool1 type=local reclaim=yeslimited
```

Resultados

Se ha completado el procesamiento de la reclamación de la agrupación de almacenamiento. La operación de protección de la agrupación de almacenamiento no se ha ejecutado, por lo que los datos de la agrupación de almacenamiento del contenedor de directorios que se ha actualizado desde la última operación de protección no están protegidos.

Qué hacer a continuación

1. Proteja los datos de la agrupación de almacenamiento de copia de contenedor emitiendo el mandato PROTECT STGPOOL y especificando el parámetro TYPE=LOCAL. El proceso de protección se ejecuta con el parámetro RECLAIM=YES predeterminado. La operación de protección lleva menos tiempo porque la reclamación ya se ha ejecutado. Por ejemplo, para proteger los datos de una agrupación de almacenamiento de copia de contenedor que se llama SPOOL1, emita el siguiente mandato:

```
protect stgpool spool1 type=local
```

También puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios que se llama SPOOL1 sin ejecutar la reclamación emitiendo el siguiente mandato:

```
protect stgpool spool1 type=local reclaim=no
```

2. Realice una copia de seguridad de la base de datos del servidor y ejecute las operaciones planificadas de mantenimiento. Para obtener instrucciones, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

Referencia relacionada:

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)
DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia de contenedor)
UPDATE STGPOOL (Definir agrupación de almacenamiento de copia de contenedor)
EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)

Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

Determine si las agrupaciones de almacenamiento de copia de contenedor cumplen los requisitos de protección frente a siniestro.

Acerca de esta tarea

Puede crear una copia externa de la agrupación de almacenamiento de copia de contenedor para la protección de recuperación ante siniestro o para satisfacer los requisitos empresariales y reglamentarios para las copias de cinta externas. Antes de decidirse por utilizar copias de cintas externas para la protección frente a siniestro, plantéese seriamente si la solución cumple con el objetivo de tiempo de recuperación.

El uso de agrupaciones de almacenamiento de copia de contenedor para la recuperación frente a siniestro es apropiado cuando la cantidad de datos del entorno es igual o menor que los valores siguientes:

- 200 TB de total de datos gestionados
- 50 TB de datos de fondo
- 37 TB de datos frontales

Total de datos gestionados

Todos los datos almacenados en la agrupación de almacenamiento de contenedores de directorios en el servidor. Esto incluye las versiones activas e inactivas de los datos. El número de versiones está determinado por las políticas de retención.

Datos de fondo

Todos los datos almacenados en la agrupación de almacenamiento de copia de contenedor.

Datos frontales

Los datos activos actuales almacenados en la agrupación de almacenamiento de copia de contenedor. Estos son los datos activos que se utilizan para restaurar datos en los nodos cliente. En caso de que se produzca un siniestro, serán necesarios todo o parte de los datos frontales para restablecer la producción. Los datos frontales son un porcentaje del total de los datos gestionados y son menores o iguales al total de datos gestionados, en función de los valores de política en uso.

Para recuperarse de un siniestro dentro de 48 horas, el entorno del sistema en el sitio de recuperación debe cumplir los requisitos de hardware mínimos para las acciones de la tabla siguiente.

Acción	Tiempo requerido	Requisitos mínimos
<p>Configure un servidor nuevo de IBM Spectrum Protect en un sitio de recuperación frente a siniestros. Para configurar el nuevo servidor, debe completar los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Suministrar discos para el servidor. 2. Restaurar el servidor desde la copia de seguridad. 3. Iniciar el servidor. 4. Actualizar las configuraciones de dispositivos y de almacenamiento. 	<p>Tiempo para restaurar el servidor: 6 horas</p>	<p>Utilice una unidad de estado sólido (SSD) para la base de datos del servidor, con los requisitos siguientes:</p> <ul style="list-style-type: none"> • Un mínimo de 100 MB por segundo de rendimiento de lectura/escritura promedio combinado • Un mínimo de 12.862 de operaciones de entrada/salida promedio por segundo (IOPS)
<p>Auditar la agrupación de almacenamiento de contenedores de directorios y reparar los datos desde la cinta. Consejo: Si el sistema cumple los requisitos mínimos de hardware, puede reparar un máximo de 50 TB de datos de fondo dentro de 48 horas.</p>	<p>Tiempo para auditar la agrupación de almacenamiento: 2 horas</p> <p>Tiempo para reparar la agrupación de almacenamiento utilizando una copia de cinta: 28 horas</p> <p>Nota: La estimación de tiempo se aplica si tiene un máximo de 200 TB del total de datos gestionados en la agrupación de almacenamiento.</p>	<p>Utilice unidades de Nearline SAS (NL-SAS), como en una configuración del servidor de blueprint media, con un mínimo de 700 MB por segundo de rendimiento de grabación para el disco de la agrupación de almacenamiento.</p> <p>Utilice la nueva generación de tecnología de cinta como, por ejemplo, LTO-7 o mejor, con un mínimo de seis unidades para permitir las operaciones de lectura simultáneas desde los volúmenes de cinta.</p>
<p>Restablezca datos en los nodos de cliente. Consejo: Si el sistema cumple los requisitos mínimos de hardware, puede restaurar un máximo de 37 TB de datos frontales dentro de 48 horas.</p>	<p>Tiempo para realizar las operaciones de restauración del cliente: 12 horas</p>	<p>Utilice unidades NL-SAS, como en una configuración del servidor de blueprint medio, con un mínimo de 10 sesiones de restauración que consiguen 3102 GB por hora.</p>

Procedimiento

1. El tipo de recuperación frente a siniestro estimado para el entorno utilizando la tabla siguiente. Determine si el tiempo de recuperación cumple los requisitos.

Tabla 1. Estimación de tiempo de recuperación para diferentes cantidades del total de datos gestionados

Objetivo de tiempo de recuperación	Total de datos gestionados (TB)	Número de horas para reparar una agrupación de almacenamiento de contenedores de directorios (First Byte Restored)	Horas hasta que se restauren los nodos de cliente (Disaster Recovery completo)
Hasta 1 al día	25	10	12
	50	13	16
	75	17	22
Hasta 2 días	100	20	26
	200	34	46
Hasta 4 días	300	48	66
	400	62	86
Más de 4 días	500	76	106

Notas:

- o Las frecuencias alcanzables dependen en gran medida de la carga de trabajo y del entorno configurado.
 - o El porcentaje de datos frontales es relativo al total de datos gestionados. Aumentar la cantidad de datos frontales aumenta el total del tiempo de recuperación. La reducción de la cantidad de datos frontales disminuye el total del tiempo de recuperación.
2. Calcule el tiempo de recuperación para el entorno mediante las fórmulas siguientes:

- o Estime el valor **Horas hasta que se repare la agrupación de almacenamiento de contenedores de directorios (First Byte Restored)**:

Time to Client First Byte Restore =
6 hours + 14 hours for every 100 TB of Total Managed Data

- o Estime el valor **Horas hasta que se restauren los nodos de cliente (Disaster Recovery completo)**:

Time to Client Restore Complete =
Time to Client First Byte Restore + ((Total Managed Data * Front-End Data) / Restore Rate)

Tasa de restauración: La velocidad a la que los clientes pueden restaurar datos desde el servidor de nuevo a su sistema local o dispositivo de almacenamiento.

3. Complete los procedimientos de prueba para la recuperación frente a siniestro para asegurarse de que las agrupaciones de almacenamiento de copia de contenedor se puedan utilizar para restaurar el entorno en un intervalo de tiempo que se ajuste a sus requisitos.

Referencia relacionada:

Reparación de agrupaciones de almacenamiento después de un siniestro

Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos

Puede almacenar datos duplicados y sin duplicar en una agrupación de almacenamiento de contenedores en la nube y restaurar los datos cuando lo necesite. Puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar uno de los siguientes protocolos y proveedores de servicios: Amazon Web Services (AWS) con Simple Storage Service (S3), IBM® Cloud Object Storage con Swift o S3 (e IBM SoftLayer), Microsoft Azure, y OpenStack con Swift utilizando Keystone versión 1 o versión 2. Las agrupaciones de almacenamiento de contenedores en la nube no se admiten en Linux on System z.

Antes de empezar

Realice los pasos siguientes:

1. Obtenga la información de configuración del proveedor de servicios en la nube:
 - o Amazon con S3 (fuera del local)
 - o Microsoft Azure
 - o IBM Cloud Object Storage con S3 (fuera del local, con IBM SoftLayer)

- o IBM Cloud Object Storage con Swift (fuera del local, con IBM SoftLayer)
 - o IBM Cloud Object Storage con S3 (en local)
 - o OpenStack con Swift (dentro o fuera del local)
2. Especifique una clase de dispositivo que se utilizará para las operaciones de copia de seguridad de base de datos. Cuando utiliza el cifrado para las agrupaciones de almacenamiento de contenedores en la nube, la clave de cifrado maestra se utiliza para proteger la clave de cifrado de la nube en una copia de seguridad de base de datos.
 - a. En la barra de menús de Centro de operaciones, seleccione Servidores.
 - b. Seleccione una fila del servidor y pulse Hacer copia de seguridad.
 - c. Seleccione una clase de dispositivo que se utilizará para las operaciones de copia de seguridad de base de datos y pulse Hacer copia de seguridad.
- Consejo: Como alternativa, utilice el mandato SET DBRECOVERY para especificar una clase de dispositivos para la copia de seguridad de base de datos.

Procedimiento

Para almacenar datos en una agrupación de almacenamiento de contenedores en la nube, complete los pasos siguientes:

1. Cree una agrupación de almacenamiento de contenedores en la nube. Debe proporcionar información de configuración que identifique el servicio en la nube.
 - a. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
 - b. En la página Agrupaciones de almacenamiento, pulse + Agrupación de almacenamiento.
 - c. Realice los pasos del asistente Añadir agrupación de almacenamiento. Seleccione Nube en local o Nube fuera de local para el tipo de almacenamiento basado en contenedor.
2. Actualice las clases de gestión y los conjuntos de políticas para que se utilice la nueva agrupación de almacenamiento. Para actualizar una clase de gestión para utilizar la nueva agrupación de almacenamiento, complete los pasos siguientes:
 - a. En la barra de menús de Centro de operaciones, pulse Servicios.
 - b. En la página Políticas, seleccione un dominio de políticas y pulse Detalles.
 - c. En la página Detalles, pulse la pestaña Conjunto de políticas.
 - d. Pulse el conmutador Configurar. Los conjuntos de políticas se pueden editar.
 - e. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
 - f. Actualice una o más clases de gestión para utilizar la nueva agrupación de almacenamiento editando el campo Destino de copia de seguridad de la tabla.
 - g. Pulse Guardar.
3. Active el conjunto de políticas cambiado completando los pasos siguientes:
 - a. Pulse Activar. Como cambiar el conjunto de políticas activo puede provocar la pérdida de datos, se muestra un resumen de las diferencias entre el conjunto de políticas activo y el nuevo conjunto de políticas.
 - b. Mire las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a las clases de gestión del conjunto de políticas actualmente activo se enlazan, después de la activación, a las clases de gestión con los mismos nombres del nuevo conjunto de políticas.
 - c. Identifique las clases de gestión del conjunto de políticas actualmente activo que no tiene contrapartidas en el nuevo conjunto de políticas, y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión los gestiona, después de la activación, la clase de gestión predeterminada en el nuevo conjunto de políticas.
 - d. Si los cambios implementados por el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.
4. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.
5. Para aprovechar el almacenamiento local, cree un directorio de agrupación de almacenamiento para esta agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY. Para obtener más información, consulte Optimización de rendimiento para almacenamiento de objetos en la nube.

Tareas relacionadas:

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS con S3

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (en local)

reparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (fuera del local)

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con Swift (fuera del local)

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack con Swift

Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube

Optimización de rendimiento para almacenamiento de objetos en la nube

Referencia relacionada:

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS con S3

Antes de configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar Amazon Web Services (AWS) fuera del local con el protocolo Simple Storage Service (S3), debe obtener información de Amazon que necesitará para el proceso de configuración.

Acerca de esta tarea

Las credenciales de cuenta de AWS son distintas de las credenciales de cuenta de Amazon. Utilice las credenciales de su cuenta de AWS cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o mediante el mandato DEFINE STGPOOL.

AWS utiliza *grupos* para almacenar datos. Los grupos de AWS se utilizan de la misma manera que los contenedores de una agrupación de almacenamiento de contenedores en la nube. IBM Spectrum Protect crea automáticamente un grupo en Amazon para una instancia de IBM Spectrum Protect y todas las agrupaciones correspondientes a esta instancia comparten dicho grupo.

Restricción: Se aplican las siguientes restricciones.

- Edite un grupo de AWS solo con IBM Spectrum Protect y no modifique los datos del grupo ni edite los valores de configuración del mismo.
- Para las agrupaciones de almacenamiento de contenedores en la nube externas que utilicen AWS con el protocolo Amazon S3, los datos están cifrados de forma predeterminada. Sin embargo, el servidor IBM Spectrum Protect no soporta el cifrado de datos mediante políticas de grupos AWS.

Procedimiento

1. Para registrar una cuenta de AWS, vaya a la página de Amazon S3 y pulse Crear una cuenta de AWS.
2. Obtenga las credenciales de AWS:
 - a. Vaya a la página de Amazon S3 y pulse Registrarse en la consola.
 - b. Seleccione su nombre y seleccione Credenciales de seguridad.
 - c. Vaya a la sección Claves de acceso para localizar los campos ID de clave de acceso y Clave de acceso secreta. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
 - Tipo de nube: `Amazon - S3 API`
 - ID de clave de acceso: `id_clave_acceso`
 - Clave de acceso secreta: `clave_acceso_secreta`
 - Región: Seleccione el punto final de la región que mejor se ajuste a su ubicación, que encontrará en la página Regiones y puntos finales de Amazon AWS. Si selecciona `Otros`, especifique un URL de punto final de región en el campo URL e incluya el protocolo, que suele ser `https://`. Normalmente, puede utilizar la región más cercana a su ubicación física para el parámetro Región. Puesto que un grupo de Amazon solo existe en una región, solo puede especificar un URL de punto final para una región. Si necesita una región GovCloud, especifique un URL de la página Puntos finales de AWS GovCloud (Estados Unidos).

Aviso: Asegúrese que utiliza únicamente el URL de punto final de AWS para el valor de la región, como `https://s3-us-west-1.amazonaws.com`. No utilice el sitio web estático que aloja el URL para este valor.
 - Nombre de grupo: Utilice el nombre de grupo predeterminado generado por el servidor, o especifique un nuevo nombre de grupo.
4. Para definir la agrupación de almacenamiento de contenedores en la nube, emita el mandato DEFINE STGPOOL con los siguientes valores:
 - CLOUDTYPE: `S3`
 - IDENTITY: `id_clave_acceso`
 - PASSWORD: `clave_acceso_secreta`
 - CLOUDURL: especifique el URL de punto final de región que mejor se ajuste a su ubicación, que encontrará en la página Regiones y puntos finales de AWS.

Normalmente, puede utilizar la región más cercana a su ubicación física para el parámetro CLOUDURL. Si necesita una región GovCloud, especifique un URL de la página Puntos finales de AWS GovCloud (Estados Unidos).

Aviso: Asegúrese que utiliza únicamente el URL de punto final de AWS para el valor de CLOUDURL, como `https://s3-us-west-1.amazonaws.com`. No utilice el sitio web estático que aloja el URL para este valor.

Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Configuración de un dispositivo compatible con Amazon S3 como agrupación de almacenamiento de contenedores en la nube

Puede configurar un dispositivo de almacenamiento que sea compatible con el protocolo Simple Storage Service (S3) de Amazon de forma que el dispositivo se pueda utilizar como una agrupación de almacenamiento IBM Spectrum Protect de contenedor en la nube.

Acerca de esta tarea

Amazon S3 utiliza *grupos* para almacenar datos. Debe crear un grupo en el dispositivo de almacenamiento compatible con S3 para que lo utilice un servidor de IBM Spectrum Protect. Después de crear el grupo, utilice las credenciales de la cuenta en el dispositivo de almacenamiento de objetos en nube compatible con Amazon S3 al configurar agrupaciones de almacenamiento con el mandato DEFINE STGPOOL.

Restricción: No cambie los datos del grupo ni edite los valores de configuración para el grupo.

Procedimiento

1. Cree un grupo en el dispositivo de almacenamiento de objetos en la nube. Siga las instrucciones de la documentación del dispositivo.
2. Cree una cuenta de usuario en el dispositivo de almacenamiento de objetos en la nube. La cuenta es utilizada por IBM Spectrum Protect para acceder al dispositivo utilizando el ID de clave de acceso y la clave de acceso secreta. Asegúrese de que la cuenta tenga permisos para almacenar datos y suprimir datos del grupo que ha creado en el paso 1. Tome nota de los valores de ID de clave de acceso y clave de acceso secreta para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Identifique el valor de URL que utilizará IBM Spectrum Protect para acceder al dispositivo de almacenamiento de objetos en la nube. Para obtener instrucciones, consulte la documentación de su dispositivo de almacenamiento de objetos en la nube.
4. Para definir la agrupación de almacenamiento de contenedores en la nube, emita el mandato DEFINE STGPOOL con los siguientes valores:

- o CLOUDTYPE: S3
- o IDENTITY: *id_clave_acceso*
- o PASSWORD: *clave_acceso_secreta*
- o CLOUDURL: `http://dirección_IP_punto_final_almacenamiento_objeto_nube` o `https://dirección_IP_punto_final_almacenamiento_objetos_nube`. Si utiliza más de un punto final, liste las direcciones IP de puntos finales separados por una barra vertical (|), sin espacios, como se muestra en el siguiente ejemplo:

```
CLOUDURL=endpoint_URL1|endpoint_URL2|endpoint_URL3
```

- o BUCKETNAME: *nombre_de_grupo_en_dispositivo*

Para optimizar el rendimiento, utilice varios puntos finales o un equilibrador de carga.

Qué hacer a continuación

Configure las agrupaciones de almacenamiento de contenedores en la nube del mismo modo que configuraría una agrupación de almacenamiento de contenedores en la nube para IBM Cloud Object Storage siguiendo las instrucciones descritas en Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para Microsoft Azure (fuera del local)

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar el sistema informático en nube Microsoft Azure, debe obtener de Microsoft la información para el proceso de configuración.

Acerca de esta tarea

IBM Spectrum Protect admite los siguientes niveles de almacenamiento de Azure:

- *Nivel de almacenamiento dinámico* para los datos a los que se accede con frecuencia

- *Nivel de almacenamiento estático* para los datos a los que se accede con menos frecuencia

Puede utilizar un nivel de almacenamiento estático para obtener un almacenamiento a largo plazo rentable. Sin embargo, es más costoso restaurar datos de un nivel de almacenamiento estático que de un nivel de almacenamiento dinámico.

Procedimiento

1. Regístrese en una cuenta de Microsoft Azure en el portal de Azure y creando una cuenta.
2. Cree una cuenta de almacenamiento. Normalmente, seleccione la ubicación más cercana al servidor de IBM Spectrum Protect más para la ubicación de la cuenta de almacenamiento.
3. Obtenga las credenciales de Azure:
 - a. Vaya al portal de Azure y pulse Cuentas de almacenamiento.
 - b. Abra una nueva cuenta de almacenamiento, vaya a la sección del contenedor del panel Blob Service y anote el valor de punto final de servicio blob para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. El punto final de servicio blob tiene un aspecto similar a estos ejemplos: `https://nombre.blob.core.windows.net` y `http://nombre.blob.core.windows.net`.
 - c. Cree una señal de firma de acceso compartido (SAS) abriendo el separador Firma de acceso compartido y complete los campos. Asegúrese de que la sección Servicios permitidos incluya Blob y que la sección Tipos de recurso permitidos incluya Contenedor y Objeto. Asegúrese de que la señal de SAS tenga permisos para leer, grabar, suprimir, listar, añadir y crear. Pulse Generar SAS.
 - d. Tome nota del valor de señal SAS para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. IBM Spectrum Protect no supervisa la fecha de caducidad de señal de SAS, por lo tanto, asegúrese de que selecciona la fecha que se adapte mejor a sus necesidades. Si la señal caduca, el servidor IBM Spectrum Protect pierde acceso a la cuenta de almacenamiento hasta que proporcione una nueva señal SAS.
Consejo: Si desea actualizar con menos frecuencia la señal SAS, establezca la fecha de caducidad dentro de unos cuantos años. Además, asegúrese de verificar los campos de fecha y hora de inicio.
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
 - o Tipo de nube: `Azure`
 - o Señal SAS: `valor_señal_SAS`. Busque una cadena similar al ejemplo siguiente:


```
?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
 - o Punto final de servicio Blob: especifique el punto final de servicio blob desde la cuenta de almacenamiento de Azure, por ejemplo, `https://nombre.blob.core.windows.net` o `http://nombre.blob.core.windows.net`.
5. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
 - o CLOUDTYPE: `Azure`
 - o PASSWORD: `valor_señal_SAS`. Busque una cadena similar al ejemplo siguiente:


```
?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
 - o CLOUDURL: especifique el punto final de servicio blob desde la cuenta de almacenamiento de Azure, por ejemplo, `https://nombre.blob.core.windows.net` o `http://nombre.blob.core.windows.net`.

Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para Azure, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con Swift (fuera del local)

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar IBM® Cloud Object Storage y IBM SoftLayer (IBM Bluemix) fuera del local utilizando Swift, debe obtener la información de configuración de la página de SoftLayer Object Storage.

Acerca de esta tarea

Utilice las credenciales de su cuenta de IBM SoftLayer cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL.

Procedimiento

1. Cree una cuenta de SoftLayer siguiendo las instrucciones de la documentación de SoftLayer.
2. Obtenga las credenciales de SoftLayer:
 - a. Vaya a la página de SoftLayer Object Storage e inicie sesión con los credenciales de su cuenta.
 - b. Seleccione la cuenta y el clúster que desea configurar.
 - c. En la sección Cuenta, pulse Ver credenciales
 - d. En la sección Credenciales de cuenta, localice los campos Punto final de autenticación pública, Nombre de usuario y Clave de API. Tome nota de los valores de esos campos para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
 - o Tipo de nube: *IBM Cloud Object Storage - Swift API (SoftLayer)*
 - o Nombre de usuario: *nombre_usuario*
 - o Contraseña: *clave_API*
 - o URL: *punto_final_autenticación_pública*
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
 - o CLOUDTYPE: *SOFTLAYER*
 - o IDENTITY: *nombre_usuario*
 - o PASSWORD: *clave_API*
 - o CLOUDURL: *punto_final_público_autenticación*

Qué hacer a continuación

Configure las agrupaciones de almacenamiento de contenedores en la nube para IBM SoftLayer siguiendo las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

reparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (fuera del local)

Puede configurar agrupaciones de almacenamiento en la nube para utilizar IBM® Cloud Object Storage fuera del local con el protocolo Simple Storage Service (S3).

Acerca de esta tarea

La implementación fuera del local de IBM Cloud Object Storage está gestionada a través de IBM SoftLayer o IBM Bluemix. En esta configuración, solo el propietario de la cuenta de Bluemix o SoftLayer puede crear grupos y administradores

Utilice las credenciales de su cuenta de IBM SoftLayer o IBM Bluemix cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL. Para obtener más información, consulte la página de SoftLayer Object Storage. Para utilizar esta configuración, seleccione Cloud Object Storage - S3 API en la página de SoftLayer Order Object Storage.

Procedimiento

1. Inicie sesión en el portal de clientes de SoftLayer.
2. Pulse el menú Almacenamiento y seleccione Almacenamiento de objetos.
3. Desde la página de almacenamiento de objetos, seleccione una cuenta S3.
4. Desde la página de almacenamiento de objetos en la nube, pulse Gestionar grupos y, continuación, el símbolo + para crear el grupo que desea utilizar con la nueva agrupación de almacenamiento de contenedores en la nube.
5. Pulse Mostrar credenciales para crear las credenciales de administrador para el nuevo grupo.
6. Pulse Añadir credencial.
7. Localice el ID de clave de acceso, la Clave de acceso secreta y el Punto final de autenticación pública. Tome nota de los valores de esos campos para que pueda utilizarlos al configurar las agrupaciones de almacenamiento. Si se encuentra dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.
8. Para configurar agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento en Centro de operaciones, seleccione Nube externa. Utilice los siguientes valores para los parámetros:
 - o Tipo de nube: *IBM Cloud Object Storage - S3 API (SoftLayer)*

- o ID de clave de acceso: *id_clave_acceso*
 - o Clave de acceso secreta: *clave_acceso_secreta*
 - o Nombre de grupo: *nombre_grupo* (desde el paso 4)
 - o URL: *punto_final_autenticación_us-geo*
Nota: Solo se necesita un punto final de proveedor de nube con esta configuración. Si todos sus servidores están dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.
9. Si configura agrupaciones de almacenamiento utilizando el mandato DEFINE STGPOOL, utilice los siguientes valores para los parámetros de mandato:
- o CLOUDTYPE: S3
 - o IDENTITY: *ID_clave_acceso*
 - o BUCKETNAME: *nombre_grupo* (del paso 4)
 - o PASSWORD: *clave_acceso_secreta*
 - o CLOUDURL: *punto_final_autenticación_us-geo*
Nota: Solo se necesita un punto final de proveedor de nube con esta configuración. Si todos sus servidores están dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.

Qué hacer a continuación

Configure las agrupaciones de almacenamiento de contenedores en la nube para IBM SoftLayer Cloud Object Storage siguiendo las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (en local)

Antes de configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar IBM® Cloud Object Storage en local con S3, debe configurar una plantilla de caja fuerte IBM Cloud Object Storage y una cuenta de usuario de IBM Cloud Object Storage y, después, obtener la información de configuración.

Acerca de esta tarea

Restricción:

Para utilizar IBM Cloud Object Storage en local con S3, asegúrese de que la versión de IBM Cloud Object Storage sea compatible con la versión de IBM Spectrum Protect.

Con IBM Spectrum Protect Versión 8.1.3, se necesita IBM Cloud Object Storage V3.7.2.31 o posterior.

Las cajas fuertes de IBM Cloud Object Storage se utilizan de la misma manera que los contenedores de una agrupación de almacenamiento de contenedores en la nube. Configure una plantilla de caja fuerte para crear rápidamente cajas fuertes con sus valores preferidos.

Después de crear una plantilla de caja fuerte, utilice las credenciales de la cuenta de usuario de IBM Cloud Object Storage para configurar las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL. El servidor utiliza el protocolo de servicio de almacenamiento simple (S3) para comunicarse con IBM Cloud Object Storage.

Consejo: Puede omitir los cuatro primeros pasos siguientes si desea configurar una caja fuerte existente utilizando el parámetro BUCKETNAME en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

Procedimiento

1. Crear una plantilla de caja fuerte:
 - a. Inicie sesión en IBM Cloud Object Storage y pulse el separador Configurar.
 - b. En el panel de navegación dsNet, expanda Agrupaciones de almacenamiento.
 - c. Seleccione la agrupación de almacenamiento de IBM Cloud Object Storage donde desea crear la plantilla de caja fuerte y pulse el enlace Agrupación de almacenamiento en la sección General.
 - d. En la sección Plantillas de caja fuerte, pulse Crear plantilla de caja fuerte.
 - e. Seleccione los valores para la plantilla de caja fuerte predeterminada. Es posible que pueda optimizar el rendimiento si no selecciona las opciones Habilitar tecnología SecureSlice o Índice de nombres habilitado y si selecciona la opción Listado de recuperación habilitado.
 - f. En la sección Despliegue, seleccione la agrupación o agrupaciones de acceso que desea utilizar para la plantilla y pulse Guardar.
2. Establezca la plantilla de caja fuerte como predeterminada para el IBM Cloud Object Storage dsNet:
 - a. Pulse la pestaña Configurar.
 - b. En la sección Configuración de plantilla de caja fuerte predeterminada, pulse Configurar.

- c. Seleccione una plantilla de caja fuerte para utilizar como predeterminada, y pulse Actualizar para establecer dicha plantilla como la predeterminada.
3. Si esta es la primera vez que configura una plantilla de caja fuerte, habilite el rol de suministro de caja de fuerte para poder crear nuevas cajas fuertes:
 - a. Pulse la pestaña Administración.
 - b. En la sección Configuración de la API de suministro, pulse Configurar.
 - c. Seleccione Crear solo o Crear y suprimir para que los usuarios puedan crear nuevas cajas fuertes mediante la API de suministro.
 - d. Pulse Actualizar para guardar los valores.
4. Utilice una cuenta de IBM Cloud Object Storage con la autoridad de administración para crear una cuenta de usuario en la instancia de IBM Cloud Object Storage en el entorno. Asegúrese de que la cuenta de usuario nueva tiene el rol de Suministrador de cuenta caja fuerte.
5. Pulse la pestaña Seguridad y seleccione la cuenta de usuario nueva.
6. Genere una clave de acceso para el usuario nuevo:
 - a. En la sección Autenticación de clave de acceso, pulse Cambiar claves.
 - b. En la página Editar claves de acceso, pulse Generar clave de acceso nueva.
 - c. Pulse Atrás.
7. En la sección Autenticación de clave de acceso, localice los valores de ID de clave de acceso y Clave de acceso secreto. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
8. Localice el valor del URL:
 - a. Pulse la pestaña Configurar.
 - b. En el panel de navegación dsNet, expanda las secciones Dispositivos y Aplicación de accesos.
 - c. Seleccione la aplicación de acceso IBM Cloud Object Storage. Verifique que la aplicación de acceso pertenece a una agrupación de acceso en la cual se ha desplegado la plantilla de caja fuerte predeterminada.
 - d. En la sección Configuración de dispositivo del dispositivo de acceso, anote el valor de Dirección IP para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. Utilice `http://` delante del valor de dirección IP para impedir errores de seguridad de certificado.
9. Si configura las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
 - o Tipo de cloud: `IBM Cloud Object Storage - S3 API`
 - o ID de clave de acceso: `id_clave_acceso`
 - o Clave de acceso secreta: `clave_acceso_secreta`
 - o Nombre de grupo: Utilice el nombre de grupo predeterminado generado por el servidor, o especifique un nuevo nombre de grupo.
 - o URL: `http://dirección_IP_acceso_almacenamiento_objetos_nube`
Importante: Si utiliza más de una aplicación de acceso, teclee la dirección IP de la aplicación de accesos y, a continuación, pulse Intro para añadir direcciones IP adicionales. Utilice varias aplicaciones de acceso o un equilibrador de carga para obtener un rendimiento óptimo.
10. Si configura las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
 - o CLOUDTYPE: `S3`
 - o IDENTITY: `ID_clave_acceso`
 - o PASSWORD: `clave_acceso_secreta`
 - o CLOUDURL: `http://dirección_IP_acceso_Cloud_Object_Store`
Importante: Si utiliza más de una aplicación de accesos, liste las direcciones IP de acceso separadas por una barra vertical (`|`), sin espacios, como por ejemplo `CLOUDURL=<URL1_acceso>|<URL2_acceso>|<URL3_acceso>`. Utilice varias aplicaciones de acceso o un equilibrador de carga para un rendimiento óptimo.

Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack con Swift

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar OpenStack en local o fuera del local con Swift, debe obtener la información de configuración del sistema OpenStack Swift.

Acerca de esta tarea

Restricción: Debe utilizar la API de OpenStack Swift Release Series Juno, Proyecto de servicio Keystone Versión 1 o 2.

Utilice las credenciales de su cuenta de OpenStack Swift al configurar las agrupaciones de almacenamiento mediante Centro de operaciones o el mandato DEFINE STGPOOL.

Procedimiento

1. Cree una cuenta de OpenStack Swift siguiendo las instrucciones de la documentación de OpenStack Swift.
2. Obtenga las credenciales de OpenStack Swift:
 - a. En el sistema OpenStack Swift, escriba el siguiente mandato:

```
swift auth -v
```
 - b. En la salida, localice los valores de `OS_AUTH_URL`, el `OS_TENANT_NAME`, el `OS_USERNAME` y la `OS_PASSWORD`. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
 - o Tipo de nube: `OpenStack Swift`
 - o Nombre de usuario: `OS_TENANT_NAME:OS_USERNAME`
 - o Contraseña: `OS_PASSWORD`
 - o URL: `OS_AUTH_URL`
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
 - o CLOUDTYPE: `SWIFT` o `V1SWIFT`
 - o IDENTITY: `OS_TENANT_NAME:OS_USERNAME`
 - o PASSWORD: `OS_PASSWORD`
 - o CLOUDURL: `URL_AUT_SO`
5. Si tiene previsto utilizar un arrendatario o un nombre de usuario específicos, anote los valores en el formato siguiente: `NOMBRE_ARRENDATARIO:NOMBRE_USUARIO`.
6. Para evitar la pérdida de datos, configure OpenStack Swift para crear réplicas de los datos que se graban en el almacén de objetos. Para obtener más información, consulte la documentación de OpenStack Swift.

Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack Swift, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube

Los datos almacenados en agrupaciones de contenedor en la nube fuera de las instalaciones están cifradas de forma predeterminada. Puede cifrar datos opcionalmente en agrupaciones de almacenamiento de contenedores en la nube fuera de las instalaciones.

Acerca de esta tarea

Para obtener información sobre el cifrado de datos de la agrupación de almacenamiento de contenedores en la nube y para consideraciones de rendimiento relacionadas con el cifrado de datos, consulte la nota técnica 1963635.

Definición de una regla de almacenamiento para los niveles en la nube

Puede definir una regla de almacenamiento para implementar los niveles en la nube, que mueven los datos de una agrupación de almacenamiento de contenedores de directorios en disco a una agrupación de almacenamiento de contenedores en la nube. La regla de almacenamiento planifica los niveles en la nube desde las agrupaciones de almacenamiento de contenedor del directorio a las agrupaciones de almacenamiento del contenedor en la nube.

Acerca de esta tarea

Puede definir reglas de almacenamiento para especificar los requisitos siguientes:

- El período de tiempo en que los datos permanecen en agrupaciones de almacenamiento de contenedor en el disco antes de moverlos en el almacenamiento en la nube.
- Si una regla de almacenamiento está activa o inactiva. Las reglas de almacenamiento se ejecutan diariamente a la hora definida en la regla de almacenamiento.

Procedimiento

1. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Reglas de niveles.
2. En la página Reglas de niveles de almacenamiento, pulse Crear regla.
3. En la página Crear regla, rellene los campos y pulse Crear.

Resultados

Cuando la regla de almacenamiento está activa, el servidor determina si las agrupaciones del contenedor del directorio de origen contienen datos lo suficientemente antiguos para moverse. El servidor mueve los datos elegibles a las agrupaciones de almacenamiento del contenedor en la nube.

Optimización de rendimiento para almacenamiento de objetos en la nube

Puede configurar IBM Spectrum Protect para almacenar datos temporalmente en uno o más directorios de agrupación de almacenamiento local durante la ingestión de datos. Los datos se han movido desde el almacenamiento local a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado.

Antes de empezar

Para optimizar el rendimiento de la copia de seguridad y el archivado, asegúrese de que esté instalada la IBM Spectrum Protect Versión 8.1.

Acerca de esta tarea

Después de definir un directorio de agrupaciones de almacenamiento, el servidor de IBM Spectrum Protect utilizará dicho directorio como un área de entrada temporal para los datos que está transfiriendo al almacenamiento de objetos de nube. El servidor utiliza un proceso en segundo plano automatizado para transferir datos del almacenamiento local en el directorio al almacenamiento de objetos de nube. No tendrá que realizar ningún paso adicional para iniciar ni gestionar este proceso de transferencia. Después de que el servidor haya movido satisfactoriamente los datos desde el almacenamiento local al almacenamiento en nube, el servidor suprimirá los datos del directorio y liberará espacio para obtener más datos entrantes.

Si los directorios de agrupaciones de almacenamiento no tienen más espacio libre, las operaciones de copia de seguridad se detendrán prematuramente. Para evitar la situación puede asignar más directorios de agrupación de almacenamiento. También puede esperar a que los datos se eliminen automáticamente de los directorios locales después de mover los datos a la nube. El número requerido de directorios de agrupaciones de almacenamiento que necesita para definir depende de la configuración de su disco en el servidor. Cuando se produzcan las copias de seguridad iniciales, el servidor distribuirá los datos en todos los directorios que haya definido.

La cantidad de espacio que necesita para el almacenamiento local se basa en la cantidad de datos que espera para realizar una copia de seguridad cada día después de la deduplicación y la compresión de datos. Si tiene una conexión de red estable al almacenamiento de objetos de nube, la cantidad de espacio necesario es similar al necesario para una copia de seguridad diaria.

Para obtener información de planificación adicional, consulte el tema para su sistema operativo:




- AIX: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube
- Linux: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube
- Windows: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube

Procedimiento

1. Cree una agrupación de almacenamiento de contenedores en la nube mediante el asistente Añadir agrupación de almacenamiento en el Centro de operaciones. De forma alternativa, cree una agrupación mediante el mandato DEFINE STGPOOL.
2. Defina uno o más directorios de agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOLDIRECTORY. Asegúrese de que cada directorio de agrupación de almacenamiento tiene su propio sistema de archivos. En sistemas Linux, utilice xfs o ext4 como sistema de archivos en lugar de ext3, porque la supresión de archivos grandes tarda más tiempo con ext3. Asegúrese de que los nuevos directorios de agrupaciones de almacenamiento no compartan el sistema de archivos raíz, ni los mismos sistemas de archivos que utilizan otros recursos de IBM Spectrum Protect, como por ejemplo la base de datos o los registros.

Referencia relacionada:

DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Gestión del espacio en las agrupaciones de almacenamiento de contenedor

Después de configurar IBM Spectrum Protect y añadir almacenamiento, gestione los datos y el espacio de la agrupación de almacenamiento de forma eficaz para asegurarse de que funcione correctamente. Utilice agrupaciones de almacenamiento de contenedores para maximizar el espacio de almacenamiento y el rendimiento del servidor.

Acerca de esta tarea

Las agrupaciones de almacenamiento de contenedores son agrupaciones de almacenamiento primario que se utilizan para la deduplicación de datos en línea, la compresión en línea y el almacenamiento en la nube.

Restricción: No puede utilizar ninguna de las siguientes funciones con agrupaciones de almacenamiento de contenedor:

- Migración
- Reclamación
- Agregación
- Proximidad
- Exportar
- Importación
- Grabación simultánea
- Copia de seguridad de agrupaciones de almacenamiento
- Volúmenes virtuales

Procedimiento

1. Para crear una agrupación de almacenamiento de contenedores de directorios, siga estos pasos:
 - a. Abra el Centro de operaciones.
 - b. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
 - c. Pulse +Agrupación de almacenamiento.
 - d. Complete los pasos del asistente Añadir agrupación de almacenamiento:
 - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
 - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
 - e. Después de configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.
2. Para obtener un rendimiento óptimo de las agrupaciones de almacenamiento de contenedor, lleve a cabo las siguientes tareas:

Tarea	Procedimiento	Más información
Proteger la agrupación de almacenamiento	<p>Cuando se crea una agrupación de almacenamiento de contenedores de directorio en el Centro de operaciones, puede configurar la protección de la agrupación de almacenamiento en la planificación que se asigna a la agrupación de almacenamiento.</p> <p>Como alternativa, utilice el mandato PROTECT STGPOOL desde el servidor de origen para hacer una copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedores de directorio.</p> <p>Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor.</p>	<ul style="list-style-type: none">○ Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio○ PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)
Reparar una agrupación de almacenamiento	<p>Cuando una agrupación de almacenamiento está protegida, puede utilizar el mandato REPAIR STGPOOL para reparar extensiones de datos dañadas. Utilice el mandato REPAIR</p>	<ul style="list-style-type: none">○ Reparación de agrupaciones de almacenamiento○ REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

	<p>STGPOOL para reparar una agrupación de almacenamiento de contenedores de directorio.</p> <p>Restricción: Si replica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorio, no puede reparar la agrupación de almacenamiento.</p>	
Suprimir contenedores	<p>Los contenedores se suprimen en el inventario a medida que los datos de archivo se eliminan o caducan.</p> <p>Utilice el mandato DEFINE STGPOOL y especifique el parámetro REUSEDELAY para controlar el tiempo que las extensiones duplicadas están asociadas a una agrupación de almacenamiento de contenedores de directorio después de que se deja de hacer referencia a la misma.</p> <p>Si un contenedor está dañado, utilice el mandato AUDIT CONTAINER para recuperar o eliminar datos.</p>	<ul style="list-style-type: none"> o DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio) o AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)
Convierta una agrupación de almacenamiento primario que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL)	<p>Puede convertir una agrupación de almacenamiento existente en una agrupación de almacenamiento de contenedores de directorio siguiendo los pasos del apartado Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor.</p> <p>Restricción: No puede convertir los siguientes tipos de agrupación de almacenamiento:</p> <ul style="list-style-type: none"> o Agrupaciones de almacenamiento primario que utilizan clases de dispositivo de acceso aleatorio (DISK) o Agrupaciones de almacenamiento de copia o Agrupaciones de almacenamiento de datos activos 	<ul style="list-style-type: none"> o CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)
Supervisar la ocupación de la agrupación de almacenamiento de contenedor	<p>Supervise la solución de almacenamiento para identificar problemas potenciales y existentes. Para obtener más información, consulte el apartado Supervisión de soluciones de almacenamiento.</p>	

- Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor
Conversión de una agrupación de almacenamiento primaria que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL) en una agrupación de almacenamiento de contenedores. Los datos que se almacenan en una agrupación de almacenamiento de contenedores pueden utilizar tanto la deduplicación de datos en línea como la compresión en línea.
- Limpieza de los datos de una agrupación de almacenamiento de origen
Para convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio, es posible que tenga que limpiar los datos o archivos dañados que están en la agrupación de almacenamiento de origen.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor

Conversión de una agrupación de almacenamiento primaria que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL) en una agrupación de almacenamiento de contenedores. Los datos que se almacenan en una agrupación de almacenamiento de contenedores pueden utilizar tanto la deduplicación de datos en línea como la compresión en línea.

Antes de empezar

Para asegurarse de que los volúmenes de una agrupación de almacenamiento y las agrupaciones de almacenamiento de copia asociadas no se reutilicen durante el proceso de conversión, especifique un valor para el parámetro REUSEDELAY en el mandato UPDATE STGPOOL. Especifique un valor para el parámetro REUSEDELAY que sea mayor que la duración de la conversión. Es posible que deba retardar la reutilización de los volúmenes por los siguientes motivos:

- Ha suprimido accidentalmente los datos durante la conversión de una agrupación de almacenamiento.
- Necesita funcionalidades de la agrupación de almacenamiento que no están disponibles en agrupaciones de almacenamiento de contenedor.

Consejo: Cuando especifica el parámetro REUSEDELAY y hay una operación de conversión en curso, hay un espacio de almacenamiento que no está disponible en la agrupación de almacenamiento de origen hasta que caduca el valor del parámetro.

Para crear una agrupación de almacenamiento de contenedores donde se traspasarán los datos, siga estos pasos:

1. En la página Agrupaciones de almacenamiento del Centro de operaciones, pulse + Agrupación de almacenamiento.
2. Realice los pasos del asistente Añadir agrupación de almacenamiento. Debe seleccionar el tipo de almacenamiento basado en contenedor que necesite.

Acerca de esta tarea

Al convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedor, elimina la necesidad de la reclamación del volumen. La omisión de las operaciones de reclamación de volúmenes puede ayudar a mejorar el rendimiento del servidor y a reducir la cantidad de hardware de almacenamiento necesario.

A medida que los archivos se convierten, las copias almacenadas en las agrupaciones de copia o en las agrupaciones de datos activos se van suprimiendo.

Restricciones:

- Si la agrupación de origen está definida como un destino de copia de seguridad, archivado o migración en un juego de políticas activo que tiene cambios pendientes, debe activar esos cambios para poder convertir la agrupación.
- Para asegurarse de que el destino especifica una agrupación de almacenamiento que no se convierte o que está llevando a cabo la conversión, debe actualizar todas las políticas que hacen referencia a la agrupación de almacenamiento de origen.
- Si la agrupación de almacenamiento de origen se ha especificado como siguiente agrupación de almacenamiento, debe actualizar el parámetro NEXTSTGPOOL del mandato UPDATE STGPOOL para especificar una agrupación de almacenamiento de acceso aleatorio o secuencial que no se esté convirtiendo.
- Los tipos de datos siguientes no son elegibles para la conversión: copias de seguridad de tablas de contenido (TOC), volúmenes virtuales y datos de NDMP (Protocolo de gestión de datos de redes). Antes de iniciar el proceso de conversión, suprima manualmente estos tipos de datos de la agrupación de almacenamiento, mueva los tipos de datos a otra agrupación de almacenamiento primaria, o permita que los tipos de datos caduquen en función de los valores de política.
- Al convertir una agrupación de almacenamiento con una clase de dispositivo FILE a una agrupación de contenedor de directorios, la agrupación de almacenamiento de destino debería ser aproximadamente un 30 % más grande que la agrupación de almacenamiento de origen. Normalmente no es necesario espacio adicional al convertir otros tipos de agrupaciones de almacenamiento.

Para obtener más información sobre las mejores prácticas de la conversión de agrupación de almacenamiento, consulte Mejores prácticas para la conversión de agrupación de almacenamiento de IBM Spectrum Protect.

- Si la agrupación de almacenamiento de origen se utiliza para almacenar copias de seguridad de TOC, asegúrese de que haya disponible otra agrupación de almacenamiento primaria para almacenar nuevas copias de seguridad de TOC. Las copias de seguridad existentes de la TOC no se mueven durante la conversión.

La agrupación de TOC debe utilizar un formato de datos NATIVE o NONBLOCK y una clase de dispositivo que no sea Centera. Para evitar que se produzcan retardos de montaje, utilice una clase de dispositivo DISK o FILE.

Procedimiento




1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione una agrupación de almacenamiento que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta, o VTL.
2. Pulse Más > Convertir y siga los pasos del asistente para Convertir agrupación de almacenamiento.
Consejo: Planifique la conversión durante al menos 2 horas para una agrupación de almacenamiento que utiliza una clase de dispositivo FILE y un mínimo de 4 horas para VTL.

Qué hacer a continuación

Cuando finalice el proceso de conversión, la agrupación de almacenamiento de origen puede contener datos dañados o datos que sean incompatibles con las agrupaciones de almacenamiento de contenedores. Para limpiar la agrupación de almacenamiento de origen, siga los pasos del apartado Limpieza de objetos tras la conversión de la agrupación de almacenamiento.

Tareas relacionadas:

Restauración de la base de datos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Limpieza de los datos de una agrupación de almacenamiento de origen

Para convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio, es posible que tenga que limpiar los datos o archivos dañados que están en la agrupación de almacenamiento de origen.

Procedimiento

Utilice las opciones siguientes para recuperar o reparar datos dañados:

- Para recuperar una versión no dañada de los datos de una copia o agrupación de almacenamiento de datos activos, utilice el mandato RESTORE STGPOOL.
- Para recuperar una versión no dañada de los datos de un servidor de réplica de destino, emita el mandato REPLICATE NODE y especifique el parámetro RECOVERDAMAGED=YES.
- Elimine los datos que no se pueden reparar después de la conversión de la agrupación de almacenamiento mediante el mandato REMOVE DAMAGED.

Es posible que el mandato REMOVE DAMAGED no elimine volúmenes que estén marcados como destruidos en la agrupación de almacenamiento de origen. Para eliminar estos volúmenes, siga estos pasos:

- a. Emita el mandato DELETE VOLUME y especifique el parámetro DISCARDDATA=YES.
 - b. Emita el mandato CONVERT STGPOOL para convertir la agrupación de almacenamiento de nuevo.
 - c. Si los datos dañados se identifican durante la conversión de la agrupación de almacenamiento, vuelva a emitir el mandato REMOVE DAMAGED.
- Lleve a cabo las tareas de análisis que se describen en la nota técnica 1666371.

Qué hacer a continuación

Tras recuperar o reparar los datos dañados, vuelva a intentar la conversión emitiendo el mandato CONVERT STGPOOL.

Para ver información sobre los archivos dañados que permanecen en la agrupación de almacenamiento de origen, emita el mandato QUERY CLEANUP.

Consejo: Si se muestra un estado Limpieza para una agrupación de almacenamiento que no contiene datos, puede suprimirla mediante el mandato DELETE STGPOOL.

Referencia relacionada:

DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)

REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)

REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)

RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)

Auditoría de un contenedor de la agrupación de almacenamiento

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre la información de base de datos y un contenedor de una agrupación de almacenamiento.

Acerca de esta tarea

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

Procedimiento

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 00000000000076c.dcf:

```
audit container c:\tsm-storage\07\00000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

Qué hacer a continuación

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Puede reparar el contenido de la agrupación de almacenamiento utilizando el mandato REPAIR STGPOOL.

Restricción: Solo puede reparar el contenido de la agrupación de almacenamiento si ha protegido dicha agrupación de almacenamiento mediante el mandato PROTECT STGPOOL.

Referencia relacionada:

➔ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

➔ QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)

Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos

Puede utilizar muchos tipos de almacenamiento para el servidor IBM Spectrum Protect. Si utiliza almacenamiento de disco de bloque, unidades de estado sólido (SSD) o sistemas de archivos conectados a red para el almacenamiento de servidor, asegúrese de que el almacenamiento cumple los requisitos.

Se aplican los siguientes requisitos al almacenamiento para la base de datos de servidor, el registro activo y el registro de archivado, para agrupaciones de almacenamiento que utilizan clases de dispositivo DISK o FILE y para agrupaciones de almacenamiento de contenedores de directorios.

El almacenamiento se puede conectar al sistema servidor mediante cualquier método que sea válido para el sistema operativo. Por ejemplo, el almacenamiento se puede conectar directamente o utilizando la tecnología de canal de fibra o iSCSI.

Debido a la variedad de sistemas de almacenamiento que pueden cumplir los requisitos del almacenamiento de servidor, no hay disponible ninguna lista de dichos dispositivos. Póngase en contacto con el proveedor si tiene preguntas sobre si un sistema cumple los requisitos de IBM Spectrum Protect.

Para obtener detalles sobre los requisitos de sistema de archivos, consulte la nota técnica 1902417. Para obtener detalles sobre los requisitos de Network File System (NFS), consulte la nota técnica 1470193.

Los sistemas de almacenamiento y de archivos deben informar sobre los resultados de confirmación y grabación de forma síncrona y precisa en el servidor de IBM Spectrum Protect. Los errores de grabación de los que no se informa o de los que se informa de forma asíncrona que hacen que los datos no se confirmen de manera permanente en el sistema de almacenamiento pueden producir corrupción de datos. La corrupción de datos puede producir anomalías operativas, incluyendo la imposibilidad de iniciar el servidor, y normalmente es necesario recuperar los datos.

Puede reducir el riesgo de corrupción de datos siguiendo las siguientes sugerencias:

Memoria caché de escritura

Los sistemas de disco utilizan memoria caché de escritura para mejorar el rendimiento del sistema. Para reducir el riesgo de corrupción de datos, el sistema de almacenamiento debe confirmar de forma fiable los datos de la memoria caché de escritura en el almacenamiento permanente.

Normalmente la memoria caché de escritura tiene una batería para evitar la pérdida de datos de la memoria caché durante cortas paradas de suministro eléctrico. Para sistemas críticos, tenga en cuenta la posibilidad de utilizar fuentes de alimentación de seguridad para proteger la memoria caché de paradas de suministro eléctrico prolongadas.

E/S directa

La E/S directa satisface la necesidad del servidor de creación de informes síncronos y precios sobre las operaciones de escritura y confirmación de datos.

Atención: No inhabilite la E/S directa en situaciones donde el método de almacenamiento en memoria caché de escritura tiene potencial para causar la pérdida de datos. Si se inhabilita la E/S directa, pueden aumentar significativamente las probabilidades de pérdida de datos dado que el sistema de archivos, además del sistema de disco, almacena en memoria caché más datos.

Réplica de almacenamiento

Los entornos que replican el almacenamiento de IBM Spectrum Protect deben utilizar características como mantenimiento de orden de escritura entre el origen (servidor local) y el destino (servidor remoto). La base de datos, el registro activo, los registros de archivado y las agrupaciones de almacenamiento deben formar parte de un grupo de consistencia. Un grupo de consistencia mantiene relaciones entre volúmenes para conservar el orden de escritura para que se puedan recuperar. Las E/S de los miembros del grupo de consistencia de destino deben escribirse en el mismo orden que en el origen y mantener las mismas características de volatilidad.

Para mantener la sincronización entre servidores de IBM Spectrum Protect en los sitios local y remoto, no inicie un servidor en el sitio remoto, excepto en una situación de migración tras error. Supervise la sincronización de datos en las ubicaciones local y remota. Si se pierde la sincronización, debe restaurar el servidor en la ubicación remota utilizando mandatos de restauración de IBM Spectrum Protect para la base de datos y las agrupaciones de almacenamiento.

Sugerencias para la configuración de almacenamiento

Si desea ver sugerencias para la configuración de almacenamiento a fin de optimizar el rendimiento, consulte los temas siguientes en la documentación de producto de la V7.1.1. La información de las listas de comprobación se puede aplicar a releases posteriores.

- Lista de comprobación de los discos de base de datos del servidor
- Lista de comprobación de los discos de registro de recuperación
- Lista de comprobación para agrupaciones de almacenamiento que utilizan clases de dispositivo DISK o FILE

Supervisión de soluciones de almacenamiento

Después de implementar una solución de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Si supervisa la solución a diario y de forma periódica, podrá identificar problemas potenciales y existentes. La información recopilada se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

Acerca de esta tarea

El método preferido para supervisar una solución es utilizar el Centro de operaciones, que proporciona el estado general y detallado del sistema en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema.

Procedimiento

1. Complete las tareas de supervisión diarias. Para obtener instrucciones, consulte Lista de comprobación de supervisiones diarias.
2. Complete las tareas de supervisión periódicas. Para obtener instrucciones, consulte Lista de comprobación de supervisiones periódicas.
3. Para verificar que el sistema cumple con los requisitos de licencia, siga las instrucciones del apartado Verificación de la conformidad de licencia.
4. Opcional: Configure los informes de correo electrónico del estado del sistema. Para obtener instrucciones, consulte el apartado Seguimiento del estado del sistema mediante informes de correo electrónico
5. Opcional: En algunos casos, es posible que desee utilizar las herramientas de supervisión avanzada para completar tareas de supervisión específicas o resolver problemas. Para seleccionar y configurar herramientas de supervisión avanzadas, consulte Selección, configuración y uso de herramientas de supervisión.

Qué hacer a continuación

Para ayudarle a diagnosticar problemas con clientes de archivado y copia de seguridad, instale servicios de gestión de cliente de IBM Spectrum Protect en cada sistema cliente de archivado y copia de seguridad que lo acepte. Cuando el servicio de gestión de cliente está instalado en un sistema, en el Centro de operaciones puede pulsar Diagnosticar para obtener ayuda para diagnosticar problemas con el cliente de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones del apartado Recopilación de información de diagnóstico con servicios de gestión de cliente de IBM Spectrum Protect .

Conceptos relacionados:

➔ Rendimiento

Tareas relacionadas:

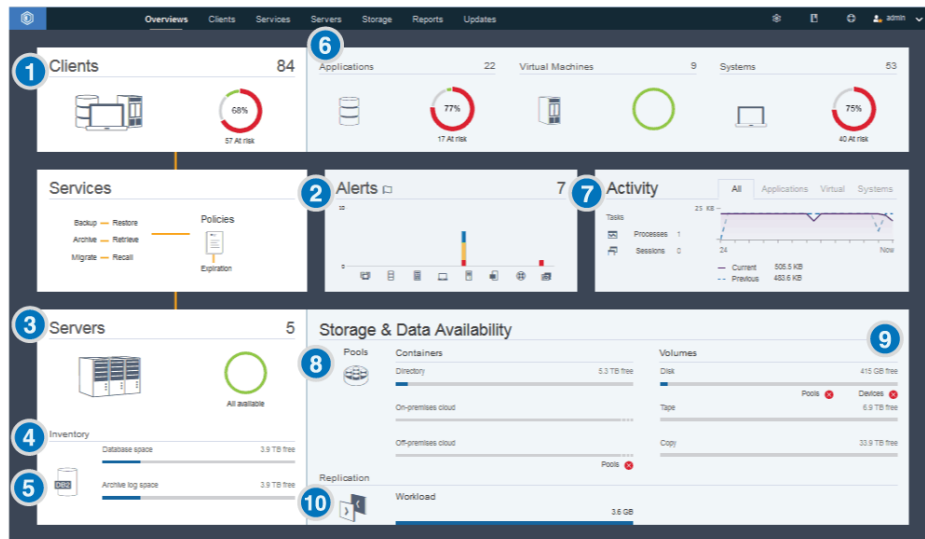
➔ Resolución de problemas


Lista de comprobación de supervisión diaria

Revise la lista de comprobación para asegurarse de que realiza las tareas de supervisión diaria importantes.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.








Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.


La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.

Tabla 1. Tareas de supervisión diarias



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>1 Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Atención: Si el porcentaje de En riesgo es mucho mayor que el habitual, puede indicar un ataque de ransomware. Un ataque de ransomware puede provocar que fallen las operaciones de seguridad, lo que pone en riesgo los clientes. Por ejemplo, si el porcentaje de clientes en riesgo normalmente está entre el 5 y el 10%, pero el porcentaje incrementa al 40 o al 50%, investigue la causa.</p> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Clientes, seleccione el cliente y pulse Detalles. 2. Para diagnosticar un problema, pulse Diagnóstico. 	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>2 Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, siga los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Alertas. 2. En la tabla Alertas, seleccione una alerta. 3. En el panel Registro de actividades, revise los mensajes. El panel muestra los mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.
<p>3 Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> 1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible. 2. Para ver información adicional, pulse el área Servidores. 3. Seleccione un servidor en la tabla Servidores y pulse Detalles. 	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione un servidor y pulse Detalles. 2. Para actualizar las propiedades de servidor, pulse Propiedades.


Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado. o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor. o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio. o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_servidor_concentrador_IBM-OC. o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio. 	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas del servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>5 Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse el área Servidores. 2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos. 	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la tabla Servidores, seleccione una fila y pulse Detalles. 2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad. <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Servidores. 2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad. <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos. 2. Emita el mandato QUERY DB: <pre>query db f=d</pre> 3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.
<p>6 Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Pulse Servidores > Mantenimiento. 2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial. 3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso. 	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>7 Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> • Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad. • Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores. 	<ul style="list-style-type: none"> • Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente. Atención: Si la cantidad de datos de la copia de seguridad es significativamente mayor que habitualmente, puede indicar un ataque de ransomware. Cuando el ransomware cifra datos, el sistema percibe que se están cambiando los datos y se realiza una copia de seguridad de dichos datos modificados. Así pues, los volúmenes de copia de seguridad aumentan. Para determinar a qué clientes afecta, pulse las pestañas Aplicaciones, Virtual o Sistemas. • Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>8 Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<p>1. Si se indican problemas en el área Almacenamiento & Disponibilidad de datos, pulse Agrupaciones para ver los detalles:</p> <ul style="list-style-type: none"> ○ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible. Atención: Si el estado es crítico, investigue la causa: <ul style="list-style-type: none"> ■ Si el índice de deduplicación de datos de una agrupación de almacenamiento disminuye significativamente, puede indicar un ataque de ransomware. Durante un ataque de ransomware, los datos se cifran y no se pueden deduplicar. Para verificar el índice de deduplicación de datos, en la tabla de agrupaciones de almacenamiento, revise el valor en la columna % de ahorro. ■ Si una agrupación de almacenamiento pasa inesperadamente a estar utilizada al 100%, puede indicar un ataque de ransomware. Para verificar el uso, revise el valor en la columna Capacidad utilizada. Pase el cursor por encima de los valores para ver los porcentajes de espacio libre y utilizado. ○ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura. <p>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</p>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento & Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  el estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> • En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes. • En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios. • Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no está disponible si está fuera de línea, si ha dejado de responder al servidor o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso. <p>Es posible que los dispositivos de cinta tengan un estado de aviso o muy grave si las unidades no están disponibles. Una unidad no está disponible si está fuera de línea, si ha dejado de responder al servidor o si su vía de acceso está fuera de línea. Es posible que un dispositivo de cinta también tenga un estado muy grave si la biblioteca está fuera de línea. Otras columnas de la tabla Dispositivos de cinta muestran el estado de la robótica de biblioteca, unidades y vías de acceso.</p> <p>Para las operaciones de copia de seguridad de cinta, compruebe que haya disponible suficientes cintas reutilizables. Si no está seguro de si el número de cintas reutilizables es suficiente, abra el cuaderno de detalles para ver el uso de cintas y una estimación de la disponibilidad de cintas reutilizables. Para abrir el cuaderno de detalles, seleccione una biblioteca en la tabla y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>10 Supervise los procesos de réplica de nodo.</p>	<ol style="list-style-type: none"> Para obtener el estado global de los procesos de réplica de nodo, vea el área Réplica en la página Centro de operaciones Descripción general. Para ver información sobre cada par de servidores replicados, pulse el área de réplica. Atención: Si percibe un aumento inesperado en el número de fallos de replicación, puede indicar un ataque de ransomware. Investigue la cause de los fallos. Para ver la cantidad de datos que se ha duplicado durante las dos últimas semanas y la velocidad de la duplicación, seleccione un par de servidores y pulse Detalles. Para ver la información de réplica para un cliente, en la página Centro de operaciones Descripción general, pulse Clientes. Vea la información en la columna Carga de trabajo de réplica. Atención: Si detecta un aumento inesperado de la carga de trabajo de replicación, puede indicar un ataque de ransomware. Investigue la cause del aumento de la carga de trabajo. 	<p>Para la supervisión avanzadas, vea la información sobre cómo ejecutar y finalizar procesos de réplica de nodos utilizando mandatos:</p> <ol style="list-style-type: none"> En la página Descripción general del Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos. Emita el mandato QUERY REPLICATION. Para obtener instrucciones, consulte QUERY REPLICATION (Consultar los procesos de réplica de nodos). Si la operación de réplica se ha completado satisfactoriamente, el valor de Total de archivos a replicar coincide con el valor de Total de archivos replicados. <p>Para mostrar mensajes que están relacionados con el proceso de réplica de un nodo en un servidor de réplica de origen o destino, siga los pasos siguientes:</p> <ol style="list-style-type: none"> En la página Visión general del Centro de operaciones pulse Servidores. Seleccione el servidor de réplica de origen o destino y pulse Detalles: <ul style="list-style-type: none"> Para ver las tareas activas, pulse Tareas activas, seleccione la tarea y verifique que se muestra el estado En ejecución. Para obtener detalles, consulte los registros de actividad relacionados. Para ver las tareas completadas, pulse Tareas completadas, seleccione la tarea y asegúrese de que se visualiza el estado Completado. Para obtener detalles, consulte los registros de actividad relacionados.

Lista de comprobación de supervisión periódica

Para asegurarse de que las operaciones se ejecutan correctamente, lleve a cabo las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.










Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>. Busque el servidor asociado al cliente. 2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>. 3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>. 4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones en QUERY ACTLOG (Consultar las anotaciones de actividades). 5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa. <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>. 2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>. 3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>. 	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento del cliente comunes</i>.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> 1. En la página <i>Centro de operaciones Descripción general</i>, pulse <i>Agrupaciones</i>. 2. Seleccione una agrupación y pulse <i>Vista rápida</i>. 3. En el área <i>Optimización de almacenamiento de datos</i>, vea la fila <i>Espacio guardado</i>. 	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores en la nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> 1. En la página <i>Descripción general de Centro de operaciones</i>, pase el ratón sobre el icono de valores  y pulse <i>Creador de mandatos</i>. 2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones en GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos para una agrupación de almacenamiento de contenedores de directorios). 3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones de QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos).

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos. 2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory query option devconfig</pre> 3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo. <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	




Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determinar si hay suficiente espacio disponible para el sistema de archivos del directorio de instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia. •  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad. <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> •  Sistemas operativos AIX •  Sistemas operativos Linux /home/tsminst1/tsminst1 •  Sistemas operativos Windows C:\tsminst1 <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Clientes. 2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente. 3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades. 4. En el área Última sesión, visualice la fila Enviado a cliente. 	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p> <p>Revise periódicamente la tabla de resumen de la actividad de SQL, que contiene estadísticas sobre sesiones de cliente. Para comparar la actividad actual con la actividad anterior, utilice una sentencia SQL SELECT. Si el nivel de actividad es significativamente diferente de actividades anteriores, puede indicar un ataque de ransomware.</p> <p>Revise periódicamente el registro de actividades. Busque mensaje de ANE que indiquen de cuántos archivos se ha realizado la copia de seguridad y cuántos se inspeccionaron. Compare el índice de deduplicación de los datos actuales con los índices anteriores. Si se realizó la copia de seguridad de un número inusualmente alto de archivos o el índice de la deduplicación de datos baja inesperado a 0, puede indicar un ataque de ransomware.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> 1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones. 2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles. 	<p>Sugerencias:</p> <ul style="list-style-type: none"> • Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. 3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>. • Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>. • Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> 1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse Detalles > Propiedades. <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores en la nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> • Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes > Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecuta más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones. 2. Seleccione una planificación y pulse Detalles. 3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila. 4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado. 5. Pulse Guardar.
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores > Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos. 2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).

Referencia relacionada:

-  [QUERY ACTLOG](#) (Consultar las anotaciones de actividades)
-  [UPDATE STGPOOL](#) (Actualizar una agrupación de almacenamiento)
-  [QUERY EXTENTUPDATES](#) (Consultar extensiones de datos actualizadas)

Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple las condiciones del acuerdo de licencia. Si comprueba el cumplimiento de forma periódica, podrá realizar un seguimiento de las tendencias del crecimiento de los datos o el uso de la unidad de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de sistema basados en los terabytes de datos almacenados en agrupaciones de almacenamiento primarias y repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

Licencia de PVU

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.



Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
Modelo frontal	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
Modelo suplementario	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad para estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
Modelo de PVU	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de conformidad con el modelo de licencias de PVU.</p>

- Evaluación de conformidad con el modelo de licencias de PVU
Si ha adquirido IBM Spectrum Protect según el modelo de licencias de unidades de valor de procesador, asegúrese que su solución cumple con los términos de licencia. Revise las estimaciones de PVU periódicamente para planificar futuras compras de licencia. Por ejemplo, si las estimaciones de PVU aumentan o tiene previsto instalar más servidores, puede adquirir más licencias.

Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener privilegios del sistema para el servidor.
- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

Procedimiento

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

Resultados

Los informes habilitados se envían según los valores especificados.

Referencia relacionada:

➔ [UPDATE ADMIN \(Actualizar un administrador\)](#)

Información relacionada:

➔ [Ejemplos de informes personalizados](#)

Selección, configuración y uso de herramientas de supervisión

Utilice el Centro de operaciones para obtener una visión general del estado del sistema y para profundizar para obtener información más detallada. En algunos casos, es posible que desee utilizar herramientas avanzadas para recopilar información de supervisión específica.





Procedimiento

Seleccione y configure las herramientas de supervisión que son adecuadas para la solución.

Tabla 1. Herramientas de supervisión

Tipo de herramienta	Casos de uso	Enlaces a más información
---------------------	--------------	---------------------------

Tipo de herramienta	Casos de uso	Enlaces a más información
Centro de operaciones	<ul style="list-style-type: none"> • Utilice la interfaz gráfica de usuario para revisar el estado del sistema y diagnosticar problemas. • Configure el Centro de operaciones para enviar informes de resumen de correo electrónico diarios. • Opcional: Personalice las alertas que se visualizan en Centro de operaciones y configure las notificaciones por correo electrónico sobre las alertas. • Opcional: Supervise el entorno de almacenamiento de forma remota visualizando la página Visión general en el navegador web de un dispositivo móvil. Por ejemplo, puede utilizar el navegador web Safari de Apple en el dispositivo iPad de Apple. También se pueden utilizar otros dispositivos móviles. <p>Consejo: Si instala servicios de gestión de cliente de IBM Spectrum Protect en un cliente de archivado y copia de seguridad, puede utilizar Centro de operaciones para obtener información sobre resolución de problemas para el cliente de archivado y copia de seguridad. El servicio de gestión de cliente se puede instalar únicamente en sistemas operativos Linux o Windows.</p>	
Mandatos administrativos de IBM Spectrum Protect	<p>Revise la información detallada. Utilice el método adecuado para la solución:</p> <ul style="list-style-type: none"> • Para visualizar los mensajes generados por el servidor y el cliente, utilice el mandato QUERY ACTLOG. Consejo: Puede ejecutar mandatos administrativos desde el creador de mandatos Centro de operaciones. • Para supervisar actividades como la migración de servidor y los inicios de sesión de cliente, utilice el cliente administrativo en la modalidad de consola. Ejecute el mandato dsmadm - consolemode. 	<ul style="list-style-type: none"> • mandatos de administración. • QUERY ACTLOG (Consultar las anotaciones de actividades) • Supervisión de actividades del servidor desde el cliente de administración • Opciones de cliente de administración

Tipo de herramienta	Casos de uso	Enlaces a más información
Registro de sucesos	Registre los mensajes de servidor y la mayoría de los mensajes de cliente como sucesos para uno o más repositorios denominados receptores.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Para obtener instrucciones sobre el uso del registro de sucesos para supervisar una solución, consulte Registro de sucesos de IBM Spectrum Protect en receptores (V7.1.1).  Sistemas operativos Linux Para obtener instrucciones sobre el registro de sucesos en un registro del sistema de Linux, consulte Registro de sucesos en el registro del sistema Linux (V7.1.4).
Consultas SQL	Cree y dé formato a consultas personalizadas de la base de datos del servidor. Por ejemplo, puede consultar la tabla de resumen de actividad SQL para ver estadísticas sobre operaciones de cliente y procesos de servidor. Para visualizar toda la información en la tabla resumen, emita el siguiente mandato desde el cliente administrativo: <pre>select * from summary</pre>	Utilización de mandatos SELECT (V7.1.1)
Herramientas del sistema operativo	Supervise y pruebe el rendimiento del sistema.	
Herramientas de supervisión de dispositivos	Supervise los dispositivos para disponibilidad, capacidad y rendimiento. Por ejemplo, utilice IBM Spectrum Control o las herramientas que se incluyen en los paquetes de hardware de dispositivo.	Para supervisar el estado general de dispositivo utilizando IBM Spectrum Control, siga las instrucciones de Supervisión del estado y la condición de los recursos. Para supervisar el rendimiento utilizando IBM Spectrum Control, siga las instrucciones de Supervisión del rendimiento de los recursos.
IBM® Tivoli Monitoring para Tivoli Storage Manager	Supervise los servidores de IBM Spectrum Protect y produzca informes históricos sobre las actividades de cliente y servidor. Consejo: El Centro de operaciones es la herramienta preferida para la supervisión. Sin embargo, Tivoli Monitoring para Tivoli Storage Manager es útil para generar informes históricos que estén basados en tecnología de IBM Cognos Business Intelligence.	Tivoli Monitoring para Tivoli Storage Manager

Gestión de operaciones

Gestionando con eficacia las operaciones de cliente y servidor, puede optimizar el rendimiento de su entorno de almacenamiento. Para empezar, supervise el entorno mediante el Centro de operaciones. A continuación, tome medidas para evitar problemas potenciales y aumentar el rendimiento.

Acerca de esta tarea

- Gestión de operaciones del servidor
Puede iniciar y detener el servidor, gestionar la capacidad de inventario y gestionar el uso de memoria y procesador. También puede optimizar la transferencia de datos entre servidores, actualizar el servidor y ajustar las actividades planificadas.
- Gestión de operaciones de cliente
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones,

que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

- **Gestión del Centro de operaciones**

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

Gestión de operaciones del servidor

Puede iniciar y detener el servidor, gestionar la capacidad de inventario y gestionar el uso de memoria y procesador. También puede optimizar la transferencia de datos entre servidores, actualizar el servidor y ajustar las actividades planificadas.

- **Detención e inicio del servidor**
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Gestión de la capacidad de inventario**
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- **Gestión del uso de la memoria y del procesador**
Asegúrese de que gestiona los requisitos de memoria y el uso de procesador para garantizar que el servidor pueda completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.
- **Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema**
Si el servidor IBM Spectrum Protect replica nodos o protege agrupaciones de almacenamiento en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Antes de habilitar la tecnología Aspera FASP, debe obtener las licencias adecuadas. Dispone de licencias tanto de evaluación como completa.
- **Planificación de la actualización del servidor**
Cuando esté disponible un fixpack o arreglo temporal, puede actualizar el servidor de IBM Spectrum Protect para beneficiarse de las mejoras del producto. Los clientes y servidores se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Ajuste de actividades planificadas**
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Mediante el ajuste de la solución, maximice los recursos del servidor y utilice de forma efectiva diferentes funciones disponibles dentro de la solución.

Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

Antes de empezar

Debe tener privilegio de sistema o de operador para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- **Inicio del servidor para tareas de mantenimiento o reconfiguración**
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Detención del servidor

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

Acerca de esta tarea

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

Procedimiento

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si hay sesiones de nodo de cliente o procesos en curso realizando los pasos siguientes:

- a. En la página Visión general de Centro de operaciones, en el área Actividades, consulte el número total de procesos y sesiones que están activos actualmente. Si el número es muy diferente al número habitual de usuarios que se muestra durante la rutina diaria de gestión del almacenamiento, observe otros indicadores de estado en el Centro de operaciones para comprobar si existe un problema.

- b. Visualice el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:

- El periodo actual, es decir, el periodo más reciente de 24 horas
- El periodo anterior, es decir, 24 horas antes del periodo actual

Si el gráfico del periodo anterior representa la cantidad de tráfico prevista, es posible que las diferencias del gráfico del periodo actual indiquen la existencia de un problema.

- c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles. Si el servidor no está registrado como un servidor concentrador o como un servidor spoke en el Centro de operaciones, obtenga información acerca de los procesos utilizando los mandatos administrativos. Emita el mandato QUERY PROCESS para consultar los procesos y obtenga información acerca de las sesiones mediante el mandato QUERY SESSION.
3. Espere a que se completen las sesiones de nodo cliente o cancele las sesiones. Para cancelar los procesos y las sesiones, realice los pasos siguientes:

- En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
- Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
- Pulse Cancelar.
- Si el servidor no está registrado como un servidor concentrador o como un servidor spoke en el Centro de operaciones, cancele las sesiones utilizando los mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancele los procesos mediante el mandato CANCEL PROCESS.
Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.

4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Inicio del servidor para tareas de mantenimiento o reconfiguración

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, `dmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

Procedimiento

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dmserv maintenance
```




Consejo: Para ver un vídeo acerca de cómo iniciar el servidor en modalidad de mantenimiento, vea Inicio de un servidor en modalidad de mantenimiento.

Qué hacer a continuación

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato `HALT`:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
 -  Sistemas operativos AIX Inicio de la instancia de servidor
 -  Sistemas operativos Linux Inicio de la instancia de servidor
 -  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

Procedimiento

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
 - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
 - Emita el mandato `EXTEND DBSPACE` para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.

Sugerencias:

 - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
 - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
 - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
 - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para

obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.

- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:

Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
 1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
 2. Detenga el servidor.
 3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
 5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la compresión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de

espacio, se debe inhabilitar la opción del servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

Referencia relacionada:

- ➔ ACTIVELOGSIZE, opción de servidor
- ➔ EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- ➔ SETOPT (Establecer una opción de servidor para actualización dinámica)

Gestión del uso de la memoria y del procesador

Asegúrese de que gestiona los requisitos de memoria y el uso de procesador para garantizar que el servidor pueda completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

Antes de empezar

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos soportados de IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

Procedimiento

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

 Sistemas operativos Linux

Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema

Si el servidor IBM Spectrum Protect replica nodos o protege agrupaciones de almacenamiento en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Antes de habilitar la tecnología Aspera FASP, debe obtener las licencias adecuadas. Dispone de licencias tanto de evaluación como completa.

Antes de empezar

La tecnología Aspera FASP se utiliza para transferir extensiones de datos desde una agrupación de almacenamiento de contenedores a un servidor remoto. Cuando la tecnología Aspera FASP está habilitada, las extensiones de datos se cifran siempre durante la transferencia, independientemente de si el protocolo de Capa de sockets seguros (SSL) está o no habilitado. Sin embargo, si desea proteger la conexión de red, habilite SSL. Para obtener información sobre SSL y cómo habilitarlo, consulte el apartado Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte.

Acerca de esta tarea

Restricciones:

- Utilice la tecnología Aspera FASP cuando la red de área amplia (WAN) muestre signos de alto nivel de pérdida de paquetes, retrasos en la transferencia de datos debidos a problemas en la red o ambos. Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Para habilitar la tecnología de Aspera FASP para las operaciones de réplica de nodos, los datos deben almacenarse en una agrupación de almacenamiento de contenedores de directorios.

Procedimiento

1. Determine si la tecnología Aspera FASP resulta adecuada para el entorno del sistema. Si se produce alguna de las siguientes condiciones, habilite la tecnología Aspera FASP:

- La media de retrasos en operaciones de transferencia de datos supera los 50 milisegundos.
- La pérdida de paquetes es superior al 0,01 %.

Las características de red pueden variar ampliamente. Es posible que pueda mejorar el rendimiento de la red mediante la habilitación de la tecnología Aspera FASP, incluso si el retraso en la transferencia de datos es de menos de 50 milisegundos y la pérdida de paquetes es inferior al 0,01 %.

2. Obtenga e instale las licencias adecuadas. Realice una de las siguientes acciones:

Obtenga e instale licencias de evaluación

Para obtener e instalar las licencias de evaluación, que caducan en 30 días, siga estos pasos:

a. Para solicitar las licencias, envíe un correo electrónico a alliances@asperasoft.com:

- Incluya el nombre de su empresa, dirección, número de teléfono y la dirección de correo electrónico del contacto principal de su empresa.
- Indique que desea una licencia de evaluación de 30 días.
- Indique el número de licencias que necesita.

Se necesita una licencia para cada servidor que se utiliza para la transferencia de datos con la tecnología Aspera FASP. Por ejemplo, si va a replicar un nodo de un servidor de origen en un servidor de destino, necesita dos licencias.

Si la solicitud de licencia se aprueba, el contacto principal recibirá un correo electrónico en un plazo de 24 horas. El correo electrónico tendrá archivos adjuntos de licencia que siguen el siguiente convenio de denominación:

xxxxx-ConnectSrv-unlim.eval.aspera-license

donde xxxxx es un número exclusivo.

b. Copie uno de los archivos de licencia en el directorio bin del servidor de origen. Seleccione un archivo de licencia. De forma predeterminada, el directorio se encuentra en la siguiente ubicación:

```
/opt/tivoli/tsm/server/bin
```

c. Copie el otro archivo de licencia en el directorio bin del servidor de destino.

d. En los servidores de origen y de destino, establezca el nivel de permiso de cada archivo de licencia en 755. Por ejemplo, si utiliza el directorio de instalación predeterminado y el número de licencia exclusivo es 47474, emita el siguiente mandato en una sola línea:

```
chmod 755 /opt/tivoli/tsm/server/bin/  
47474-ConnectSrv-unlim.eval.aspera-license
```

Obtenga e instale licencias completas

Para obtener e instalar las licencias completas e ilimitadas, que no caducan, siga estos pasos:

a. Adquiera el producto Transferencia de datos de datos de velocidad de IBM Spectrum Protect. El número de identificación del producto es 5725-Z10. Puede obtener el producto desde Passport Advantage.

Se necesita una instancia de Transferencia de datos de datos de velocidad de IBM Spectrum Protect para cada servidor que se utilice para transferir los datos con la tecnología Aspera FASP. Por ejemplo, si va a replicar un nodo de un servidor de origen en un servidor de destino, necesita dos licencias de Transferencia de datos de datos de velocidad de IBM Spectrum Protect.

b. Instale Transferencia de datos de datos de velocidad de IBM Spectrum Protect en cada servidor utilizando el asistente de instalación.

Restricción: Si faltan licencias necesarias o han caducado, las operaciones para replicar nodos y proteger las agrupaciones de almacenamiento mediante la tecnología Aspera FASP fallarán.

3. Opcional: Valide la configuración de Aspera FASP emitiendo el mandato `VALIDATE ASPERA`. Puede utilizar el mandato `VALIDATE ASPERA` para verificar que el entorno del sistema se haya configurado correctamente para Aspera FASP y para verificar que se hayan instalado licencias válidas. Además, puede utilizar el mandato para comparar la velocidad de la productividad de la red con Aspera FASP y la tecnología de TCP/IP.

Qué hacer a continuación

Para habilitar la tecnología Aspera FASP, siga los pasos del apartado Optimización de la transferencia de datos mediante la habilitación de la tecnología Aspera FASP.

- Optimización de la transferencia de datos mediante la habilitación de la tecnología Aspera FASP
Si utiliza un servidor remoto para la protección de la agrupación de almacenamiento o la réplica de nodos y tiene problemas de red, es posible que desee optimizar la transferencia de datos mediante la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

Planificación de la actualización del servidor

Cuando esté disponible un fixpack o arreglo temporal, puede actualizar el servidor de IBM Spectrum Protect para beneficiarse de las mejoras del producto. Los clientes y servidores se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

Acerca de esta tarea

Siga estas directrices:




- El método recomendado consiste en actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

Procedimiento

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor es compatible con otros componentes como, por ejemplo, clientes de biblioteca y agentes de almacenamiento. Consulte el apartado nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

Qué hacer a continuación

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Mediante el ajuste de la solución, maximice los recursos del servidor y utilice de forma efectiva diferentes funciones disponibles dentro de la solución.

Procedimiento

1. Supervise el rendimiento del sistema de forma periódica para asegurarse de que las tareas de copia de seguridad de cliente y de mantenimiento de servidor se completan satisfactoriamente. Siga las instrucciones de la sección Supervisión de soluciones de almacenamiento.
2. Opcional: Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, revise la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
 - El número de clientes aumenta.
 - La cantidad de datos de los que se hace copia de seguridad aumenta.
 - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución está funcionando en el nivel esperado. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
 - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
 - b. Pulse Detalles.
 - c. Desde la página de Resumen de cliente, revise la actividad de Copia de seguridad y Réplica para identificar los riesgos.Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.

4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:

- a. Proteger agrupaciones de almacenamiento.
- b. Replicar datos de nodo.
- c. Realizar una copia de seguridad de la base de datos.
- d. Ejecutar el proceso de caducidad para eliminar copias de seguridad de cliente y copias de archivo de archivado del almacenamiento de servidor.

Consejo: Planificar que las tareas de mantenimiento se inicien a una hora adecuada y en la secuencia correcta. Por ejemplo, planificar tareas de réplica después de que las copias de seguridad de cliente se completen satisfactoriamente.

- Traslado de clientes de un servidor a otro

Para que no se agote el espacio de un servidor o para resolver problemas de carga de trabajo, es posible que tenga que trasladar los nodos de cliente de un servidor a otro.

Conceptos relacionados:

📄 Rendimiento

Tareas relacionadas:

📄 Eliminación de datos duplicados (V7.1.1)

Gestión de operaciones de cliente

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

Acerca de esta tarea

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- **Modificación del ámbito de una copia de seguridad de cliente**
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.
- **Evaluación de errores en registros de errores de cliente**
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- **Detención y reinicio del aceptador de cliente**
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- **Restablecimiento de contraseñas**
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- **Poner fuera de servicio un nodo cliente**
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor IBM Spectrum Protect, pero ya no se utilizaba la estación de trabajo, puede dejar fuera de servicio la estación de trabajo.
- **Desactivación de datos para liberar espacio de almacenamiento**
En algunos casos, puede desactivar datos que están almacenados en el servidor IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.
- **Gestión de actualizaciones del cliente**
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

Modificación del ámbito de una copia de seguridad de cliente

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Acerca de esta tarea

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Si desea obtener más información al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción dominio. Siga las instrucciones de Opción de cliente de dominio.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

Evaluación de errores en registros de errores de cliente

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

Antes de empezar

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de cliente se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte el apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes.

Procedimiento

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de cliente se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
 1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
 2. Pulse Detalles.
 3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
 4. Revise los mensajes de registro recuperados.

Sugerencias:

 - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
 - Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

 5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si servicio de gestión de cliente no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

Detención y reinicio del aceptador de cliente

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

Acerca de esta tarea

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para garantizar las operaciones planificadas se pueden llevar a cabo en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

Procedimiento

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, siga los pasos siguientes:
 - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764      1   0 16:26:35 ?                0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```


- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Para detener el servicio aceptador de cliente, siga los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, siga los pasos siguientes:
 - a. Pulse Inicio > Herramientas administrativas > Servicios.
 - b. Efectúe doble pulsación en el servicio aceptador de cliente.
 - c. Pulse Iniciar y Aceptar.

Referencia relacionada:

 Resolución de problemas de planificación del cliente

Restablecimiento de contraseñas

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

Procedimiento

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre_nodo* especifica el nodo cliente y *nueva_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:

1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre_nodo* especifica el nombre del nodo y *nueva_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor IBM Spectrum Protect, pero ya no se utilizaba la estación de trabajo, puede dejar fuera de servicio la estación de trabajo.

Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
 1. En la página Visión general del Centro de operaciones, pulse Clientes y seleccione el cliente.
 2. Pulse Más > Poner fuera de servicio.
- Para poner fuera de servicio un nodo cliente utilizando un mandato administrativo, complete los pasos siguientes:
 1. Determine si el nodo cliente se ha configurado para la réplica de nodo emitiendo el mandato QUERY NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, ejecute el siguiente mandato:

```
query node austin format=detailed
```

Revise el campo de salida de Estado de réplica.

2. Si el nodo cliente se ha configurado para la réplica, elimine el nodo cliente de la réplica emitiendo el mandato REMOVE REPLNODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
remove replnode austin
```

3. Realice una de las siguientes acciones:

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o varios espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o varios espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Qué hacer a continuación

Vea si aparecen mensajes de error, que se pueden ver en la interfaz de usuario o en la salida del mandato, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo cliente está fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
 - El estado FUERA DE SERVICIO indica que el nodo está fuera de servicio.
 - Un valor nulo indica que el nodo no está fuera de servicio.
 - El estado PENDIENTE indica que se está realizando el proceso de colocar el nodo fuera de servicio o que dicho proceso ha fallado.

Consejo: Si desea determinar el estado de un proceso de colocación fuera de servicio pendiente, emita el mandato siguiente:

```
query process
```

3. Revise la salida del mandato:
 - Si se muestra el estado del proceso de servicio de retirada de servicio, significa que el proceso está en curso. Por ejemplo:

```
query process
```

Proceso proceso	Descripción proceso	Estado proceso
----- 3 desactivados	----- NODO FUERA DE SERVICIO	----- Número de objetos de copia de seguridad para el nodo NODE1: 8 objetos desactivados.

- Si no se muestra el estado del proceso de servicio de retirada de servicio y no ha recibido ningún mensaje de error, significa que el proceso está incompleto. Un proceso puede estar incompleto si los archivos que asociados al nodo aún no se han desactivado. Una vez desactivados los archivos, vuelva a ejecutar el proceso de colocación fuera de servicio.
- Si no se muestra el estado del proceso de servicio de retirada de servicio y recibe un mensaje de error, significa que el proceso ha fallado. Vuelva a ejecutar el proceso de retirada de servicio.

Referencia relacionada:

- [DECOMMISSION NODE \(Dejar fuera de servicio un nodo de cliente\)](#)
- [DECOMMISSION VM \(Dejar fuera de servicio una máquina virtual\)](#)
- [QUERY NODE \(Consultar nodos\)](#)
- [REMOVE REPLNODE \(Eliminar un nodo de cliente de la réplica\)](#)

Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar datos que están almacenados en el servidor IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

Referencia relacionada:

- [DEACTIVATE DATA \(Desactivar datos para un nodo de cliente\)](#)

Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos soportados de IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad del agente de almacenamiento y el cliente de biblioteca con los servidores configurados como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

Procedimiento

Para actualizar el software, siga las instrucciones que figuran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"> • Planificación de actualizaciones de cliente
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> • Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot para VMware • Instalación y actualización de IBM Spectrum Protect Snapshot para Windows
IBM Spectrum Protect para bases de datos	<ul style="list-style-type: none"> • Actualización de Data Protection for SQL Server • Instalación de Data Protection for Oracle • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2 • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> • Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> • Instalación y actualización de Data Protection para VMware • Instalación de protección de datos para Microsoft Hyper-V

Gestión del Centro de operaciones

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que

detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.

- Reinicio del asistente de configuración inicial

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

- Cambio del servidor concentrador

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

- Restauración de la configuración a un estado de preconfiguración

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Adición y eliminación de servidores spoke

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

Acerca de esta tarea

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke
Puede eliminar un servidor spoke del Centro de operaciones.

Adición de un servidor de radio

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

Antes de empezar

La comunicación entre el servidor spoke y el servidor concentrador debe protegerse mediante el uso del protocolo de Seguridad de la capa de transporte (Transport Layer Security - TLS). Para proteger las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

Procedimiento

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
 - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
 - Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor de radio.

Eliminación de un servidor spoke

Puede eliminar un servidor spoke del Centro de operaciones.

Acerca de esta tarea

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.

- Desea que el servidor spoke quede fuera de servicio.

Procedimiento

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre_grupo* representa el nombre del grupo supervisado y *nombre_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```

Consejo: Si una definición de servidor se suprime inmediatamente después de que se elimine el servidor del grupo supervisado, la información de estado del servidor puede permanecer en el Centro de operaciones indefinidamente.


Para evitar este problema, espere a que pase el intervalo de recopilación de estados antes de suprimir la definición de servidor. El intervalo de recopilación de estados se muestra en la página Valores del Centro de operaciones.

Inicio y detención del servidor web


El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.

Procedimiento


1. Detener el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation_dir/ui/Utils* donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:


```
./stopserver.sh
```

-  Sistemas operativos Linux Emita el mandato siguiente:

```
service opscenter.rc stop
```

-  Sistemas operativos Windows Desde la ventana Servicios, detenga el servicio IBM Spectrum Protect Centro de operaciones.

2. Inicie el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation_dir/ui/Utils* donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

```
./startserver.sh
```

-  Sistemas operativos Linux Emita los mandatos siguientes:

Inicie el servidor:


```
service opscenter.rc start
```

Reinicie el servidor:

```
service opscenter.rc restart
```

Determine si se está ejecutando el servidor:

```
service opscenter.rc status
```

-  Sistemas operativos Windows Desde la ventana Servicios, inicie el servicio IBM Spectrum Protect Centro de operaciones.

Reinicio del asistente de configuración inicial

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

Antes de empezar

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:







- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.

Acerca de esta tarea

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

Procedimiento

1. Detenga el servidor web de Centro de operaciones.
 2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde *installation_dir* representa el directorio en el que está instalado Centro de operaciones:
 -  Sistemas operativos AIX  Sistemas operativos Linux *installation_dir*/ui/Liberty/usr/servers/guiServer
 -  Sistemas operativos Windows *installation_dir*\ui\Liberty\usr\servers\guiServer
- Por ejemplo:
-  Sistemas operativos AIX  Sistemas operativos Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
 -  Sistemas operativos Windows c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. En el directorio guiServer, elimine el archivo serverConnection.properties.
 4. Inicie el servidor web Centro de operaciones.
 5. Abra el Centro de operaciones.
 6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
 7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

Cambio del servidor concentrador

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

Procedimiento

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

Tareas relacionadas:

Reinicio del asistente de configuración inicial

Restauración de la configuración a un estado de preconfiguración

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Procedimiento

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
 - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
 - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: *IBM-OC-nombre_servidor_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

- e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

- f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restaure los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.





Tareas relacionadas:

Reinicio del asistente de configuración inicial

Inicio y detención del servidor web

Configuración de bibliotecas de cintas virtuales

Una biblioteca de cintas virtuales (VTL) no utiliza medios de cinta físicos. Cuando implemente el almacenamiento de VTL, puede superar la capacidad de una biblioteca de cintas físicas. La capacidad para definir varios volúmenes y unidades puede proporcionar mayor flexibilidad al entorno de almacenamiento.

- Consideraciones sobre el uso de las bibliotecas de cintas virtuales
Existen ciertas consideraciones para la definición de una biblioteca como una biblioteca de cintas virtuales (VTL), incluidas las mejoras en el rendimiento y la configuración de su hardware.
- Agregar una biblioteca de cintas virtuales a su entorno
Defina una biblioteca de cintas virtuales (VTL) para beneficiarse de las ventajas en el rendimiento del montaje y la escalabilidad.
- Definir todas las unidades y vías de acceso de una biblioteca
Puede utilizar el mandato `PERFORM LIBACTION` para configurar una biblioteca SCSI o una biblioteca virtual de cintas (VTL) en un solo paso.
-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad
Configure una biblioteca VTL o SCSI que contenga dos unidades de cinta LTO.
-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Configure una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad
Puede configurar una biblioteca con varios tipos de dispositivos de unidad, como por ejemplo, una biblioteca StorageTek L40 que contiene una unidad DLT y una unidad LTO Ultrium.

Consideraciones sobre el uso de las bibliotecas de cintas virtuales

Existen ciertas consideraciones para la definición de una biblioteca como una biblioteca de cintas virtuales (VTL), incluidas las mejoras en el rendimiento y la configuración de su hardware.

Acerca de esta tarea

La definición de una VTL en el servidor de IBM Spectrum Protect puede ayudar a mejorar el rendimiento, ya que el servidor maneja el proceso de puntos de montaje para las VTL de modo diferente que para las bibliotecas de cintas reales. Las limitaciones físicas del hardware de cintas reales no se aplican a una VTL, ofreciendo opciones para una mejor escalabilidad.

Puede utilizar una VTL para cualquier biblioteca de cintas virtuales siempre que se cumplan las siguientes condiciones:

- No hay soportes combinados implicados en la VTL. Sólo se emula en la biblioteca un tipo y una generación de unidades y soportes.
- Cada servidor y agente de almacenamiento con acceso a la VTL tiene vías de acceso definidas para todas las unidades de la biblioteca.

Si no se cumple alguna de estas condiciones, podrá reducirse o anularse cualquier ventaja derivada de definir una biblioteca VTL en el servidor de IBM Spectrum Protect.

Las VTL son compatibles con versiones anteriores tanto de los clientes de biblioteca como de los agentes de almacenamiento. El cliente de biblioteca o el agente de almacenamiento no se ve afectado por el tipo de biblioteca que se utiliza para el almacenamiento. Si las condiciones de las vías de acceso y los soportes combinados se cumplen para una biblioteca SCSI, puede definirse o actualizarse como `LIBTYPE=VTL`.

- Capacidad de almacenamiento para las bibliotecas de cintas virtuales
Como las bibliotecas de cintas virtuales (VTL) no tienen las limitaciones físicas que tiene el hardware de cinta real, su capacidad de almacenamiento es más flexible.
- Configuración de unidades para las bibliotecas de cintas virtuales
La configuración de unidades en una biblioteca de cintas virtual (VTL) es variable, dependiendo de las necesidades del entorno.

Capacidad de almacenamiento para las bibliotecas de cintas virtuales

Como las bibliotecas de cintas virtuales (VTL) no tienen las limitaciones físicas que tiene el hardware de cinta real, su capacidad de almacenamiento es más flexible.

El concepto de capacidad de almacenamiento en una biblioteca de cintas virtual es distinto de la capacidad en un hardware de cinta física. En una biblioteca de cintas física, cada volumen tiene una capacidad definida, y la capacidad de la biblioteca se define en términos del número total de volúmenes en la biblioteca. Por otro lado, la capacidad de una VTL se define en términos del espacio de disco total disponible. Puede aumentar o disminuir el número y el tamaño de los volúmenes en el disco.

Esta variabilidad afecta a lo que significa quedarse sin espacio en una VTL. Por ejemplo, un volumen en una VTL puede quedarse sin espacio antes de alcanzar su capacidad asignada si el total de discos subyacentes se queda sin espacio. En esta situación, el servidor puede recibir un mensaje de fin de volumen sin otro aviso, lo que provoca errores de copia de seguridad.

Cuando se producen errores de copia de seguridad y falta de espacio, normalmente todavía hay espacio de disco disponible en la VTL. Se oculta en volúmenes que no se están utilizando. Por ejemplo, los volúmenes que se suprimen lógicamente o se devuelven a estado reutilizable en el servidor de IBM Spectrum Protect solo se suprimen en la base de datos del servidor. No se notifica a la VTL, que mantiene el tamaño completo del volumen como asignado en sus cálculos de capacidad.

Para evitar errores de falta de espacio, asegúrese de que toda biblioteca SCSI que actualice a LIBTYPE=VTL se actualice con el parámetro RELABELSCRATCH establecido en YES. La opción RELABELSCRATCH permite al servidor sobrescribir la etiqueta de cualquier volumen que se suprima y devolver el volumen al estado reutilizable en la biblioteca. El parámetro RELABELSCRATCH se establece de forma predeterminada en YES para cualquier biblioteca definida como una VTL.

Referencia relacionada:

UPDATE LIBRARY (Actualizar una biblioteca)

Configuración de unidades para las bibliotecas de cintas virtuales

La configuración de unidades en una biblioteca de cintas virtual (VTL) es variable, dependiendo de las necesidades del entorno.

La mayoría de los entornos VTL utilizar tantas unidades como sea posible para maximizar el número de operaciones de cinta simultáneas. Un montaje de cinta individual en un entorno VTL suele ser más rápido que un montaje de cinta física. No obstante, el uso de muchas unidades aumenta la cantidad de tiempo que requiere el servidor de IBM Spectrum Protect cuando se solicita un montaje. El proceso de selección tarda más tiempo, ya que aumenta el número de unidades definidas en un objeto de biblioteca individual en el servidor. Los montajes de cintas virtuales puede tardar el mismo tiempo o más que los montajes de cintas físicas, dependiendo del número de unidades en VTL.

Para obtener mejores resultados al crear unidades, compruebe con el proveedor de VTL las recomendaciones específicas para el dispositivo. Si se requieren más de 300-500 unidades para cada VTL, puede hacer una partición lógica del VTL en varias bibliotecas y asignar unidades a cada biblioteca. Las configuraciones de hardware de SAN y sistema operativo pueden imponer limitaciones en el número de dispositivos que pueden utilizarse en la biblioteca VTL.

Agregar una biblioteca de cintas virtuales a su entorno

Defina una biblioteca de cintas virtuales (VTL) para beneficiarse de las ventajas en el rendimiento del montaje y la escalabilidad.

Acerca de esta tarea

Las VTL se identifican utilizando el mandato DEFINE LIBRARY y especificando el parámetro LIBTYPE=VTL. Dado que una biblioteca VTL funcionalmente interactúa con el servidor igual que una biblioteca SCSI, puede utilizar el mandato UPDATE LIBRARY para cambiar el tipo de biblioteca de una biblioteca SCSI que ya esté definida. No es necesario volver a definir la biblioteca.

Procedimiento

- Añadir una biblioteca VTL nueva. Defina la biblioteca como una VTL en el servidor, como se muestra en el ejemplo siguiente:

```
define library chester libtype=vtl
```

Así se establece la nueva biblioteca VTL y se habilita la opción RELABELSCRATCH para volver a etiquetar los volúmenes que han sido suprimidos y devueltos al estado reutilizable.

- Actualizar una biblioteca SCSI a una VTL. Si dispone de una biblioteca SCSI y desea cambiarla a una VTL, utilice el mandato UPDATE LIBRARY para cambiar el tipo de biblioteca:

```
update library calzone libtype=vtl
```

Solo puede emitir este mandato si la biblioteca que se va a actualizar está definida con el parámetro LIBTYPE=SCSI.

Referencia relacionada:

DEFINE LIBRARY (Definir una biblioteca)

UPDATE LIBRARY (Actualizar una biblioteca)

Definir todas las unidades y vías de acceso de una biblioteca

Puede utilizar el mandato PERFORM LIBACTION para configurar una biblioteca SCSI o una biblioteca virtual de cintas (VTL) en un solo paso.

Acerca de esta tarea

Si está configurando o modificando el entorno de hardware y debe crear o cambiar un gran número de definiciones de unidades, el mandato PERFORM LIBACTION puede facilitarle mucho esta tarea. Puede definir una nueva biblioteca y, a continuación, definir todas las unidades y vías de acceso a las unidades. O, si dispone de una biblioteca existente que desea suprimir, puede suprimir todas las unidades existentes y sus vías de acceso en un solo paso.

El parámetro PREVIEW le permite ver la salida de los comandos antes de que se procesen para verificar la acción que desea realizar. Si define una biblioteca, ya tiene que haber una vía de acceso a la biblioteca definida si desea especificar el parámetro PREVIEW. No puede utilizar los parámetros PREVIEW y DEVICE de forma conjunta.

El mandato PERFORM LIBACTION solo se puede utilizar para bibliotecas SCSI y VTL. Si está definiendo unidades y vías de acceso a la biblioteca, la opción SANDISCOVERY debe estar admitida y habilitada. La biblioteca de cintas tiene que poder devolver la asociación de dirección del número de serie.


Procedimiento

Para configurar una biblioteca VTL denominada ODIN, complete estos pasos:

1. Defina la biblioteca.

```
define library odin libtype=vtl
```

2. Defina dos unidades y sus vías de acceso para la nueva biblioteca, ODIN.

 Sistemas operativos AIX

```
perform libaction odin action=define device=/dev/lb3 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=/dev/
lb3 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/mt2
```

 Sistemas operativos Linux

```
perform libaction odin action=define device=/dev/tsm SCSI/lb3 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=/dev/tsm SCSI/lb3
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/tsm SCSI/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/tsm SCSI/mt2
```

 Sistemas operativos Windows

```
perform libaction odin action=define device=lb0.0.0.2 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=lb0.0.0.2
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=mt0.1.0.2 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=mt0.2.0.2
```

Referencia relacionada:

DEFINE LIBRARY (Definir una biblioteca)

DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)

PERFORM LIBACTION (Definir o suprimir todas las unidades y vías de acceso de una biblioteca)

Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad

Configure una biblioteca VTL o SCSI que contenga dos unidades de cinta LTO.

Acerca de esta tarea

Este procedimiento es un ejemplo de cómo configurar una biblioteca SCSI automatizada que contiene dos unidades en el sistema servidor. La biblioteca no está compartida con otros servidores de IBM Spectrum Protect o con agentes de almacenamiento, y está conectada normalmente al sistema de servidor mediante tablas SCSI.

En esta configuración, ambas unidades de la biblioteca son el mismo tipo de dispositivo. Defina una clase de dispositivo. El procedimiento es el mismo tanto para las bibliotecas SCSI como para las VTL, excepto el paso para definir la biblioteca. En las bibliotecas SCSI, defina la biblioteca con `libtype=scsi`. En las bibliotecas VTL, puede definir la biblioteca con `libtype=vtl`.

Procedimiento


1. Defina una biblioteca SCSI denominada AUTODTLIB.

```
define library autoltolib libtype=scsi
```

Si la biblioteca tiene un lector de código de barras y desea etiquetar cintas automáticamente antes de darlas de alta, puede establecer el parámetro AUTOLABEL en YES. Por ejemplo:

```
define library autoltolib libtype=scsi autolabel=yes
```

2. Defina una vía de acceso desde el servidor a la biblioteca.

 Sistemas operativos AIX

```
define path server1 autoltolib srctype=server desttype=library
device=/dev/lb3
```

 Sistemas operativos Linux

```
define path server1 autoltolib srctype=server desttype=library
device=/dev/tsmscsi/lb3
```

 Sistemas operativos Windows


```
define path server1 autoltolib srctype=server desttype=library
device=lb0.0.0.3
```

3. Defina las unidades de la biblioteca. Las dos unidades pertenecen a la biblioteca AUTODTLIB.

```
define drive autoltolib drive01
define drive autoltolib drive02
```

Consejo: Puede utilizar el mandato PERFORM LIBACTION para definir unidades y vías de acceso para una biblioteca en un paso.

4. Defina una vía de acceso del servidor a cada unidad.

 Sistemas operativos AIX

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=/dev/mt4
```



```
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=/dev/mt5
```

Sistemas operativos Linux

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=/dev/tmscsi/mt4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=/dev/tmscsi/mt5
```

Sistemas operativos Windows

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.5
```

Si no ha especificado la dirección de elemento al definir la unidad, el servidor consulta ahora la biblioteca para obtener la dirección de elemento predeterminada correspondiente a la unidad.

5. Defina una clase de dispositivo denominada AUTODLT_CLASS para las dos unidades de la biblioteca AUTODLTLIB.

```
define devclass autolto_class library=autodlplib devtype=lto
```

6. Defina una agrupación de almacenamiento denominada AUTOLTO_POOL asociada a la clase de dispositivo denominada AUTOLTO_CLASS.

```
define stgpool autolto_pool autolto_class maxscratch=20
```

7. Etiquete y dé de alta todos los volúmenes de biblioteca.

```
label libvolume autoltolib search=yes labelsource=barcode checkin=scratch
```

8. Verifique las definiciones emitiendo los siguientes mandatos:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

Referencia relacionada:

DEFINE DEVCLASS (Definir una clase de dispositivo)

DEFINE LIBRARY (Definir una biblioteca)

DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)

Ejemplo: Configure una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad

Puede configurar una biblioteca con varios tipos de dispositivos de unidad, como por ejemplo, una biblioteca StorageTek L40 que contiene una unidad DLT y una unidad LTO Ultrium.

Acerca de esta tarea

Este procedimiento es un ejemplo de cómo configurar una biblioteca SCSI automatizada que contiene dos unidades en el sistema servidor. La biblioteca no está compartida con otros servidores de IBM Spectrum Protect o con agentes de almacenamiento, y está conectada normalmente al sistema de servidor mediante cables SCSI.

En esta configuración, las unidades son tipos de dispositivos distintos. Defina una clase de dispositivo para cada tipo de dispositivo de unidad. Las unidades con tipos de dispositivos distintos están admitidas en una única biblioteca si define una clase de dispositivo para cada tipo de unidad. Si emplea esta configuración, debe incluir el formato específico del tipo de dispositivo de la unidad utilizando el parámetro FORMAT con un valor distinto de DRIVE.


El procedimiento es el mismo tanto para las bibliotecas SCSI como para las VTL, excepto el paso para definir la biblioteca. En las bibliotecas SCSI, defina la biblioteca con libtype=scsi. En las bibliotecas VTL, puede definir la biblioteca con libtype=vtl.

Procedimiento

1. Defina una biblioteca SCSI denominada MIXEDLIB.

```
define library mixedlib libtype=scsi
```

2. Defina una vía de acceso desde el servidor a la biblioteca.

 Sistemas operativos AIX

```
define path server1 mixedlib srctype=server desttype=library  
device=/dev/lb3
```

 Sistemas operativos Linux

```
define path server1 mixedlib srctype=server desttype=library  
device=/dev/tmsmcsi/lb3
```


 Sistemas operativos Windows

```
define path server1 mixedlib srctype=server desttype=library  
device=lb0.0.0.3
```

3. Defina las unidades en la biblioteca. Ambas unidades pertenecen a la biblioteca MIXEDLIB.

```
define drive mixedlib dlt1  
define drive mixedlib lto1
```

4. Defina una vía de acceso del servidor a cada unidad. El parámetro DEVICE especifica el nombre del controlador de dispositivo para la unidad, que es el nombre de archivo especial de dispositivo.

 Sistemas operativos AIX

```
define path server1 dlt1 srctype=server desttype=drive  
library=mixedlib device=/dev/mt4  
define path server1 lto1 srctype=server desttype=drive  
library=mixedlib device=/dev/mt5
```

 Sistemas operativos Linux

```
define path server1 dlt1 srctype=server desttype=drive  
library=mixedlib device=/dev/tmsmcsi/mt4  
define path server1 lto1 srctype=server desttype=drive  
library=mixedlib device=/dev/tmsmcsi/mt5
```

 Sistemas operativos Windows

```
define path server1 drive01 srctype=server desttype=drive  
library=auto1tolib device=mt0.0.0.4  
define path server1 drive02 srctype=server desttype=drive  
library=auto1tolib device=mt0.0.0.5
```

Si no ha especificado la dirección de elemento al definir la unidad, el servidor consulta ahora la biblioteca para obtener la dirección de elemento correspondiente a la unidad.

5. Defina clases de dispositivo.

Importante: No utilice el formato DRIVE, que es el valor predeterminado. Como las unidades son de tipos diferentes, el servidor utiliza la especificación de formato para seleccionar una unidad. El uso del formato DRIVE en una biblioteca de medios mixtos puede tener consecuencias imprevisibles.

```
define devclass dlt_class library=mixedlib devtype=dlt format=dlt40  
define devclass lto_class library=mixedlib devtype=lto format=ultriumc
```

6. Defina agrupaciones de almacenamiento asociadas a las clases de dispositivo.

```
define stgpool lto_pool lto_class maxscratch=20  
define stgpool dlt_pool dlt_class maxscratch=20
```

7. Etiquete y dé de alta todos los volúmenes de biblioteca.

```
label libvolume mixedlib search=yes labelsource=barcode checkin=scratch
```

8. Verifique las definiciones emitiendo los siguientes comandos:

```
query library  
query drive  
query path  
query devclass  
query stgpool  
query libvolume
```

Protección de servidores de archivos NAS

Puede configurar y gestionar un entorno de copia de seguridad que proteja su servidor de archivos de almacenamiento adjunto de red (NAS).

Puede utilizar el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad de IBM Spectrum Protect o IBM Spectrum Protect Snapshot para realizar una copia de seguridad y restaurar un servidor de archivos NAS como se describe en la tabla siguiente.

Producto	Descripción
Servidor de IBM Spectrum Protect	<p>Para realizar una copia de seguridad y restaurar datos del servidor de archivos NAS utilizando el servidor de IBM Spectrum Protect, debe tener instalado IBM Spectrum Protect Extended Edition.</p> <p>Puede configurar el servidor de IBM Spectrum Protect para utilizar el protocolo de gestión de datos de redes (NDMP) para realizar una copia de seguridad y restaurar los datos como se describe en los siguientes temas de esta sección.</p> <p>Para proteger los sistemas de archivos NetApp grandes, también puede configurar IBM Spectrum Protect para que utilice la característica NetApp SnapMirror to Tape (también denominada SMTape). SnapMirror to Tape utiliza una copia de datos a nivel de bloque para la copia de seguridad, que es un método más rápido que una copia de seguridad completa tradicional NDMP y se puede utilizar si las copias de seguridad completas de NDMP no resultan prácticas.</p> <p>Para obtener información sobre el uso de SnapMirror to Tape para realizar una copia de seguridad y restaurar datos, consulte Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape.</p>
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<p>Puede configurar el cliente de archivado y copia de seguridad para realizar una copia de seguridad y restaurar los datos del servidor de archivos utilizando el protocolo Network File System (NFS) o Common Internet File System (CIFS).</p> <p>Para obtener información sobre cómo utilizar el cliente de archivado y copia de seguridad para realizar una copia de seguridad y restaurar datos, consulte Copia de seguridad y restauración de datos con los clientes de archivado y copia de seguridad.</p>
IBM Spectrum Protect Snapshot	<p>Puede utilizar IBM Spectrum Protect Snapshot para realizar una copia de seguridad y restaurar los datos del servidor de archivos utilizando las tecnologías de instantáneas avanzadas de los sistemas de almacenamiento.</p> <p>Para obtener información sobre cómo utilizar IBM Spectrum Protect Snapshot para hacer una copia de seguridad de los datos y restaurarlos, consulte Visión general de IBM Spectrum Protect Snapshot para UNIX y Linux o bien Visión general de IBM Spectrum Protect Snapshot for VMware.</p>

- **Requisitos de NDMP**
Para utilizar NDMP para operaciones con servidores de archivos NAS, debe tener instalado IBM Spectrum Protect Extended Edition y el entorno de servidor de archivos debe cumplir determinados requisitos.
- **Gestión de operaciones NDMP**
Existen diversas actividades de administrador para las operaciones NDMP.
- **Configuración de IBM Spectrum Protect para operaciones NDMP**
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad y recuperar datos en los servidores de archivos NAS utilizando NDMP. El procedimiento de configuración varía dependiendo de si tiene previsto realizar una copia de seguridad de los datos desde un servidor de archivos NAS en clúster o no de clúster.
- **Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP**
Después de configurar IBM Spectrum Protect para operaciones NDMP, está listo para empezar a utilizar NDMP.
- **Copia de seguridad y restauración en nivel de archivo para operaciones NDMP**
Al realizar una copia de seguridad de los datos utilizando NDMP, puede especificar que el servidor de IBM Spectrum Protect recopile y almacene información de nivel de archivo en una tabla de contenido (TOC).
- **Operaciones de copia de seguridad y restauración a nivel de directorio**
Si tiene un sistema de archivos NAS grande, al iniciar una copia de seguridad a nivel de directorios se reducen los tiempos de copia de seguridad y restauración y se proporciona más flexibilidad en la configuración de copias de seguridad NAS. Al definir los espacios de archivos virtuales, la copia de seguridad del sistema de archivos se debe partir en varias operaciones de copia de seguridad NDMP y varias unidades de cintas. También puede utilizar distintas planificaciones de copia de seguridad con el fin de realizar una copia de seguridad de subárboles de un sistema de archivos.
- **Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape**
Puede realizar una copia de seguridad de sistemas de archivos NetApp grandes utilizando la característica NetApp SnapMirror to Tape (también denominada SMTape). Si se usa una copia de datos a nivel de bloque para copia de seguridad, el método SnapMirror to Tape es más rápido que una copia de seguridad completa tradicional NDMP y se puede usar si las copias de seguridad completas de NDMP no resultan prácticas.

- Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra. Cuando el servidor de IBM Spectrum Protect inicia una operación de copia de seguridad NDMP en un transportador de datos Celerra, la copia de seguridad de un sistema de archivos grande puede tardar varias horas en realizarse. Sin los puntos de comprobación integrados de Celerra, los cambios que se producen en el sistema de archivos se graban en la imagen de copia de seguridad.
- Réplica de los nodos NAS
Puede replicar un nodo NAS que utiliza NDMP para operaciones de copia de seguridad. Antes de configurar la operación de réplica, revise las restricciones que se aplican.

Requisitos de NDMP

Para utilizar NDMP para operaciones con servidores de archivos NAS, debe tener instalado IBM Spectrum Protect Extended Edition y el entorno de servidor de archivos debe cumplir determinados requisitos.

servidor de archivos NAS

IBM Spectrum Protect debe admitir el sistema operativo del servidor de archivos. Para obtener información sobre los servidores de archivos de NAS admitidos, consulte nota técnica 1054144.

El servidor de archivos NAS debe admitir la combinación del modelo de servidor de archivos y el sistema operativo. Para obtener información más específica, consulte la documentación del producto para el servidor de archivos de NAS.

Bibliotecas de cintas

Este requisito sólo es necesario para una copia de seguridad en un dispositivo NAS conectado localmente. El servidor de IBM Spectrum Protect da soporte a los siguientes tipos de bibliotecas para las operaciones que utilizan NDMP:

SCSI

Una biblioteca SCSI puede conectarse directamente al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Cuando se conecta la biblioteca directamente al servidor de IBM Spectrum Protect, ese servidor controla las operaciones de la biblioteca pasando los mandatos SCSI directamente a la biblioteca. Cuando se conecta la biblioteca directamente al servidor de archivos NAS, el servidor de IBM Spectrum Protect controla la biblioteca pasando los mandatos SCSI a la biblioteca mediante el servidor de archivos NAS.

ACSLs

Una biblioteca ACSLS (software de biblioteca del sistema de cartuchos automatizados) puede conectarse directamente solo al servidor de IBM Spectrum Protect. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud de biblioteca a través de TCP/IP al servidor de control de la biblioteca.

Restricción: El servidor de IBM Spectrum Protect no incluye soporte de biblioteca externa para la biblioteca ACSLS cuando la biblioteca se utiliza para las operaciones NDMP.

VTL

Una biblioteca virtual de cintas (VTL) se puede conectar directamente al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Una biblioteca virtual de cintas es esencialmente igual que una biblioteca SCSI, pero mejorada para las características de biblioteca virtual de cintas y con un mejor rendimiento de montaje.

Si está definiendo una VTL, el entorno no puede incluir medios combinados. Las vías de acceso deben estar definidas entre todas las unidades de la biblioteca y todos los servidores definidos incluidos los agentes de almacenamiento que utiliza la biblioteca. Si no se cumplen estas condiciones, el rendimiento general puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad.

349X

Una biblioteca 349X se puede conectar directamente al servidor de IBM Spectrum Protect. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud de biblioteca a través de TCP/IP al gestor de biblioteca.

Compartición de biblioteca: El servidor IBM Spectrum Protect que realiza operaciones NDMP puede ser un gestor de biblioteca, tanto para una biblioteca ACSLS, SCSI, VTL o para una biblioteca 349X, pero no puede ser un cliente de biblioteca. El servidor de IBM Spectrum Protect también puede ser un cliente de biblioteca, en una configuración en la que el servidor de archivos NAS envía datos al servidor mediante TCP/IP, en lugar de a una biblioteca de cintas conectada al servidor de archivos. Si la ejecución de las operaciones de NDMP en el servidor de IBM Spectrum Protect que es un gestor de biblioteca, el servidor de biblioteca que debe controlar directamente y no mediante mandatos pasados a través de un servidor de archivos NAS.

Unidades de cintas

Una unidad de cintas sólo es necesaria para realizar una copia de seguridad en un dispositivo NAS conectado localmente. El servidor de archivos NAS debe poder acceder a las unidades. Una biblioteca de dispositivos distintos no admite un dispositivo NAS. El servidor de archivos NAS y el sistema operativo deben admitir las unidades para operaciones de copia de seguridad. Para obtener soporte completo de dispositivos para NDMP, consulte la documentación del producto del servidor de archivos NAS.

Compartición de unidades: El servidor de IBM Spectrum Protect y uno o más servidores de archivos NAS pueden compartir unidades de cintas. Asimismo, cuando se conecta una biblioteca SCSI, VTL o 349X al servidor y no al servidor de archivos NAS, las unidades se pueden compartir entre uno o varios servidores de archivos NAS: Las unidades también se pueden compartir por uno o varios clientes de almacenamiento y clientes de biblioteca de IBM Spectrum Protect.

Reservas de unidad: Cuando las unidades de cintas se conectan a dispositivos NAS y se especifica el parámetro RESETDRIVES=YES para el mandato DEFINE LIBRARY, se aplican las siguientes limitaciones:

- Si un servidor IBM Spectrum Protect y un dispositivo NAS comparten una unidad de cintas, la preferencia de reserva de unidad se soporta cuando el dispositivo NAS soporta la reserva persistente y está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
- Si una unidad está conectada únicamente a un dispositivo NAS y no se comparte con un servidor de IBM Spectrum Protect, no se admite la preferencia de reserva de unidad. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

Consulte con los fabricantes de hardware la compatibilidad de combinaciones específicas de un servidor de archivos NAS con dispositivos de cintas y dispositivos con conexión a la SAN.

Consejo: IBM Spectrum Protect admite NDMP Versión 4 para todas las operaciones NDMP. IBM Spectrum Protect sigue siendo compatible con todas las copias de seguridad NDMP y las operaciones de restauración con un dispositivo NAS que ejecuta NDMP con versión 3. El servidor de IBM Spectrum Protect negocia el nivel de protocolo superior (bien la versión 3 o la versión 4) con el servidor NDMP cuando establece una conexión NDMP. Si experimenta problemas con la versión 4 es posible que desee utilizar la versión 3.

- Interfaces para operaciones NDMP
Puede usar diversas interfaces para ejecutar operaciones NDMP. Para planificar una operación NDMP, utilice el mandato BACKUP NODE o RESTORE NODE y cree una planificación para procesar el mandato.
- Formatos de datos para operaciones de copia de seguridad NDMP
Los datos que se copian utilizando NDMP no tienen el mismo formato que los datos que se utilizan para las operaciones de copia de seguridad de IBM Spectrum Protect típicas. El servidor de archivos NAS controla el formato de los datos de copia de seguridad.

Interfaces para operaciones NDMP

Puede usar diversas interfaces para ejecutar operaciones NDMP. Para planificar una operación NDMP, utilice el mandato BACKUP NODE o RESTORE NODE y cree una planificación para procesar el mandato.

Interfaces de cliente:

- Cliente de línea de mandatos de copia de seguridad/archivado (en un sistema Windows, AIX de 64 bits u Oracle Solaris de 64 bits)
- Cliente Web

Interfaces de servidor:

- Consola del servidor
 - Línea de mandatos en el cliente de administración
- Consejo: Todos los ejemplos de las operaciones NDMP utilizan mandatos de servidor.

La interfaz de cliente web de IBM Spectrum Protect, disponible con el cliente de copia de seguridad/archivado, muestra gráficamente los sistemas de archivos del servidor de archivos NAS. La función de cliente no es necesaria, pero puede utilizar las interfaces de cliente para operaciones NDMP. La función de cliente es el método preferido para las operaciones de restauración de nivel de archivo. Para obtener más información acerca de las operaciones de restauración, consulte Copia de seguridad y restauración en nivel de archivo para operaciones NDMP.

IBM Spectrum Protect le solicitará un ID de administrador y una contraseña cuando realice funciones NDMP a través de cualquiera de las dos interfaces de cliente. Para obtener más información sobre la instalación y la activación de interfaces de cliente, consulte Instalación de los clientes de copia de seguridad y archivado de IBM Spectrum Protect.

Para poder utilizar el cliente de copia de seguridad/archivado o el cliente web de IBM Spectrum Protect con el fin de realizar operaciones NAS, los nombres del sistema de archivos en el dispositivo NAS deben incorporar una barra inclinada (/) como primer carácter. Esta restricción no afecta a las operaciones NAS que se hayan iniciado desde la línea de mandatos del servidor de IBM Spectrum Protect.

Formatos de datos para operaciones de copia de seguridad NDMP

Los datos que se copian utilizando NDMP no tienen el mismo formato que los datos que se utilizan para las operaciones de copia de seguridad de IBM Spectrum Protect típicas. El servidor de archivos NAS controla el formato de los datos de copia de seguridad.

Los datos que se han copiado en una biblioteca que está directamente conectada al servidor de archivos deben direccionarse a una agrupación de almacenamiento con el formato de datos adecuado. Cuando define una agrupación de almacenamiento para

operaciones NDMP, especifique uno de los siguientes formatos de datos:

- NETAPPDUMP, si el servidor de archivos NAS es un dispositivo NetApp o un dispositivo IBM® System Storage de serie N.
- CELERRADUMP, si el servidor de archivos de NAS es un dispositivo EMC Celerra.
- NDMPDUMP para los demás dispositivos.

Los datos que se copian a través de la red en la jerarquía de IBM Spectrum Protect local pueden direccionarse a cualquier agrupación de almacenamiento primario de acceso aleatorio o acceso secuencial. No obstante, el formato de los datos no cambia.

Gestión de operaciones NDMP

Existen diversas actividades de administrador para las operaciones NDMP.

- Gestión de los nodos del servidor de archivos NAS
Puede consultar, actualizar, renombrar y eliminar nodos de servidor de archivos NAS.
- Gestión de los transportadores de datos utilizados en las operaciones NDMP
Puede consultar, actualizar y suprimir los transportadores de datos que defina para servidores de archivos NAS.
- Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP
Si ya utiliza una unidad para operaciones IBM Spectrum Protect, puede dedicar dicha unidad para operaciones NDMP.
- Gestión de agrupaciones de almacenamiento para operaciones NDMP
Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales.
- Gestión de tablas de contenido
Puede utilizar diversos mandatos para gestionar diferentes aspectos de sus contenidos de datos.
- Impedir que se cierren las conexiones NDMP de larga ejecución inactivas
Para impedir que los cortafuegos cierren las conexiones NDMP que son de larga ejecución pero están inactivas, puede habilitar el estado activo de TCP (protocolo de control de transmisiones) en las conexiones de control NDMP.

Gestión de los nodos del servidor de archivos NAS

Puede consultar, actualizar, renombrar y eliminar nodos de servidor de archivos NAS.

Procedimiento

Utilice uno de los siguientes mandatos para gestionar los nodos del servidor de archivos NAS:

mandato	Procedimiento
QUERY NODE	Para consultar un nodo, emita el mandato QUERY NODE con los parámetros adecuados. Por ejemplo, si desea consultar el nodo NAS NASNODE1, emita el siguiente mandato: <code>query node nasnode1 type=nas</code>
UPDATE NODE	Para actualizar un nodo, emita el mandato UPDATE NODE con los parámetros adecuados. Por ejemplo, si ha creado un nuevo dominio de políticas denominado NASDOMAIN para nodos NAS y desea actualizar el nodo NASNODE1 para incluirlo en el nuevo dominio, emita el siguiente mandato: <code>update node nasnode1 domain=nasdomain</code>

mandato	Procedimiento
RENAME NODE	<p>Para cambiar el nombre de un nodo NAS, también debe cambiar el nombre del transportador de datos NAS correspondiente; ambos deben tener el mismo nombre.</p> <p>Por ejemplo, para cambiar el nombre NASNODE1 por NAS1, realice los pasos siguientes:</p> <ol style="list-style-type: none"> 1. Suprima todas las vías de acceso entre el transportador de datos NASNODE1 y las bibliotecas, así como entre el transportador de datos y NASNODE1 y las unidades. 2. Suprima el transportador de datos definido para el nodo NAS. 3. Para cambiar el nombre NASNODE1 por NAS1, emita el mandato siguiente: <pre>rename node nasnode1 nas1</pre> 4. Defina el transportador de datos mediante el nuevo nombre de nodo. En este ejemplo, debe definir un nuevo transportador de datos llamado NAS1 con los mismos parámetros utilizados para definir NASNODE1. <p>Importante: Cuando defina un nuevo transportador de datos para un nodo cuyo nombre ha cambiado, asegúrese de que el nombre del transportador de datos coincida con el nuevo nombre de nodo. Y, además asegúrese de que los parámetros del nuevo transportador de datos sean duplicados de los parámetros del transportador de datos original. Si existen discrepancias entre un nombre de nodo y un nombre de transportador de datos o entre los parámetros del nuevo transportador de datos y los parámetros del transportador de datos original, es posible que no pueda establecer una sesión con el servidor de archivos NAS.</p> 5. Para las bibliotecas SCSI o 349X, defina una vía de acceso entre el transportador de datos NAS y una biblioteca sólo si la biblioteca de cintas está conectada física y directamente al servidor de archivos NAS. 6. Defina vías de acceso entre el transportador de datos NAS y las unidades utilizadas para operaciones NDMP.
REMOVE NODE	<p>Para eliminar un nodo, siga estos pasos:</p> <ol style="list-style-type: none"> 1. Suprima las definiciones de espacios de archivos virtuales del nodo. 2. Suprima todas las vías de acceso entre el transportador de datos y las bibliotecas, así como entre el transportador de datos y las unidades. 3. Suprima el nodo. Por ejemplo, si desea eliminar un nodo denominado NAS1, emita el siguiente mandato: <pre>remove node nas1</pre>

Referencia relacionada:

- QUERY NODE (Consultar nodos)
- UPDATE NODE (Actualizar atributos del nodo)
- RENAME NODE (Cambiar el nombre de un nodo)
- REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)

Gestión de los transportadores de datos utilizados en las operaciones NDMP

Puede consultar, actualizar y suprimir los transportadores de datos que defina para servidores de archivos NAS.

Procedimiento

Utilice uno de los mandatos siguientes para gestionar los transportadores de datos:

Mandato	Procedimiento
QUERY DATAMOVER	Para consultar un transportador de datos, emita el mandato QUERY DATAMOVER con los parámetros adecuados. Por ejemplo, si desea consultar el transportador de datos NASNODE1, emita el siguiente mandato: <code>query datamover nasnode1</code>
UPDATE DATAMOVER	Para actualizar un transportador de datos, emita el mandato UPDATE DATAMOVER con los parámetros adecuados. Por ejemplo, si cierra un servidor de archivos NAS para realizar tareas de mantenimiento y desea poner el transportador de datos fuera de línea, emita el siguiente mandato: <code>update datamover nasnode1 online=no</code>
DELETE DATAMOVER	Para suprimir un transportador de datos, emita el mandato DELETE DATAMOVER. Por ejemplo, si desea suprimir el transportador de datos NASNODE1, emita el siguiente mandato: <code>delete datamover nasnode1</code> Restricción: Si el transportador de datos tiene una vía de acceso a una biblioteca y suprime o desactiva el transportador de datos, imposibilitará el acceso a la biblioteca.

Referencia relacionada:

QUERY DATAMOVER (visualizar definiciones de un transportador de datos)

UPDATE DATAMOVER (Actualizar un transportador de datos)

DELETE DATAMOVER (Suprimir un transportador de datos)

Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP

Si ya utiliza una unidad para operaciones IBM Spectrum Protect, puede dedicar dicha unidad para operaciones NDMP.

Procedimiento

Elimine el acceso al servidor de IBM Spectrum Protect suprimiendo la definición de vía de acceso. Por ejemplo, si el nombre de servidor es SERVER1 y la unidad es NASDRIVE1, emita el siguiente mandato:

```
delete path server1 nasdrive1 srctype=server desttype=drive library=naslib
```

Gestión de agrupaciones de almacenamiento para operaciones NDMP

Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales.

Se aplican las siguientes directrices y restricciones a las agrupaciones de almacenamiento de tipo NETAPPDUMP, CELERRADUMP, y NDMPDUMP generadas por las operaciones NDMP:

- Puede consultar y actualizar agrupaciones de almacenamiento, pero no puede actualizar el parámetro DATAFORMAT.
- No es posible designar una agrupación de almacenamiento CENTERA, de contenedor de directorios o de contenedor en la nube como agrupación de destino de operaciones NDMP.
- Se recomienda mantener agrupaciones de almacenamiento separadas para datos de proveedores de NAS diferentes, aunque el formato de datos de ambos sea NDMPDUMP.
- Los siguientes parámetros de mandato DEFINE STGPOOL y UPDATE STGPOOL se pasan por alto puesto que no se admiten jerarquías de agrupaciones de almacenamiento ni operaciones de reclamación o migración para estas agrupaciones de almacenamiento:
 - MAXSIZE
 - NEXTSTGPOOL
 - LOWMIG
 - HIGHMIG

- o MIGDELAY
- o MIGCONTINUE
- o RECLAIMSTGPOOL
- o OVFLLOCATION

Importante: Asegúrese de que no utiliza de forma accidental agrupaciones de almacenamiento definidas para operaciones NDMP en operaciones de IBM Spectrum Protect tradicionales. Sea especialmente precavido cuando asigne al nombre de agrupación de almacenamiento el valor del parámetro DESTINATION del mandato DEFINE COPYGROUP. Si el destino no es una agrupación de almacenamiento con el formato de datos adecuado, la operación de copia de seguridad fallará.

Gestión de tablas de contenido

Puede utilizar diversos mandatos para gestionar diferentes aspectos de sus contenidos de datos.

Acerca de esta tarea

El mandato SET TOCLOADRETENTION puede utilizarse para especificar el número aproximado de minutos que una tabla de contenido sin referencia permanecerá cargada en la base de datos de IBM Spectrum Protect. El valor de retención de TOC en el servidor de IBM Spectrum Protect determina cuánto tiempo se conservará una tabla de contenido cargada en la base de datos tras el último acceso a la información de la tabla de contenido.

Dado que la información de la tabla de contenido (TOC) se carga en tablas de bases de datos temporales, esta información se pierde si se detiene el servidor, aunque no haya transcurrido el período de retención de la tabla de contenido (TOC). Durante la instalación, el tiempo de retención se establece en 120 minutos. Utilice el mandato QUERY STATUS para ver el tiempo de retención de la tabla de contenido.

Emita el mandato QUERY NASBACKUP para visualizar información acerca de los objetos de imagen de sistema de archivos de los que se ha efectuado una copia de seguridad para un nodo NAS y un espacio de archivos específicos. Al emitir el mandato, puede visualizar todas las imágenes de copia de seguridad generadas por NDMP y si cada imagen tiene una TOC correspondiente.

Consejo: El servidor de IBM Spectrum Protect puede almacenar una copia de seguridad completa que exceda el número de versiones especificado si esa copia de seguridad completa tiene copias de seguridad diferenciales dependientes. Las copias de seguridad de NAS completas con copias de seguridad diferenciales dependientes se comportan igual que cualquier otro archivo base con subarchivos dependientes. Debido al tiempo de retención especificado en el valor RETEXTRA, la copia de seguridad completa de NAS no caducará y la versión se mostrará en la salida de un mandato QUERY NASBACKUP. Para obtener información sobre la configuración de las políticas de retención de datos, consulte el apartado Personalización de políticas.

Utilice el mandato QUERY TOC para visualizar archivos y directorios en una imagen de copia de seguridad generada por NDMP. Emitiendo el mandato de servidor QUERY TOC, puede visualizar todos los directorios y archivos de una única tabla de contenido (TOC) especificada. Se accederá a la tabla de contenido (TOC) especificada de una agrupación de almacenamiento cada vez que se emita el mandato QUERY TOC, ya que este mandato no carga la información de la tabla de contenido (TOC) en la base de datos de IBM Spectrum Protect. A continuación, utilice el mandato RESTORE NODE con el parámetro FILELIST para restaurar archivos individuales.

Impedir que se cierren las conexiones NDMP de larga ejecución inactivas

Para impedir que los cortafuegos cierren las conexiones NDMP que son de larga ejecución pero están inactivas, puede habilitar el estado activo de TCP (protocolo de control de transmisiones) en las conexiones de control NDMP.




Acerca de esta tarea

El servidor de IBM Spectrum Protect inicia las conexiones de control para dispositivos de NAS durante las operaciones NDMP de copia de seguridad o restauración. Estas conexiones de control pueden permanecer abiertas e inactivas durante un largo período de tiempo. Por ejemplo, supongamos que el mismo dispositivo NAS pone en marcha dos operaciones NDMP. La conexión de control para una operación NDMP puede permanecer abierta, pero inactiva, si la operación requiere un recurso, por ejemplo, una unidad de cintas o volumen secuencial, que está siendo utilizado por la otra operación NDMP.

Algún software de cortafuegos se configura para cerrar automáticamente conexiones de red que llevan inactivas un período específico de tiempo. Si existe un cortafuegos entre un servidor de IBM Spectrum Protect y un dispositivo NAS, es posible que el cortafuegos pueda cerrar las conexiones de control NDMP inesperadamente y provocar que la operación NDMP falle.

El servidor de IBM Spectrum Protect proporciona un mecanismo, el estado activo de TCP, que se puede habilitar para impedir que las conexiones de larga ejecución inactivas se cierren. Si el estado activo de TCP está habilitado, los paquetes pequeños se envían a través de la red, a intervalos predefinidos, al socio de conexión.

Restricción: Para evitar errores, no habilite el estado activo TCP en determinados tipos de entornos. Un ejemplo son los entornos en los que no existen cortafuegos entre el servidor de IBM Spectrum Protect y un dispositivo NAS. Otro ejemplo son los entornos con cortafuegos que toleran conexiones inactivas de larga ejecución. Habilitar el estado activo de TCP en este tipo de entornos puede causar que una conexión inactiva se cierre por error si el socio de conexión no responde temporalmente a los paquetes de estado activo de TCP.

- **Habilitar el estado activo de TCP**
Para habilitar el estado activo de TCP, que mantiene abiertas las conexiones NDMP, utilice la opción de servidor NDMPENABLEKEEPALIVE.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especificar tiempo de inactividad de conexión para el estado activo de TCP
Para especificar el período de tiempo de inactividad de la conexión, en minutos, antes de que se envíe el primer paquete de estado activo de TCP, utilice la opción del servidor NDMPKEEPIDLEMINUTES.

Habilitar el estado activo de TCP

Para habilitar el estado activo de TCP, que mantiene abiertas las conexiones NDMP, utilice la opción de servidor NDMPENABLEKEEPALIVE.




Procedimiento

Agregue la opción al archivo de opciones del servidor dsmserv.opt:

```
ndmpenablekeepalive yes
```

Referencia relacionada:

NDMPENABLEKEEPALIVE

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Especificar tiempo de inactividad de conexión para el estado activo de TCP

Para especificar el período de tiempo de inactividad de la conexión, en minutos, antes de que se envíe el primer paquete de estado activo de TCP, utilice la opción del servidor NDMPKEEPIDLEMINUTES.

Procedimiento

Agregue la opción al archivo de opciones del servidor dsmserv.opt:

```
ndmpkeepidleminutes minutes
```

Referencia relacionada:

NDMPKEEPIDLEMINUTES

Configuración de IBM Spectrum Protect para operaciones NDMP

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad y recuperar datos en los servidores de archivos NAS utilizando NDMP. El procedimiento de configuración varía dependiendo de si tiene previsto realizar una copia de seguridad de los datos desde un servidor de archivos NAS en clúster o no de clúster.



- **Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster**
Antes de configurar IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster, registre la licencia necesaria.
- **Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno en clúster de NetApp**
Puede realizar una copia de seguridad de los datos de un clúster de NetApp en un dispositivo de cinta conectado directamente o en servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Puede realizar una copia de seguridad del clúster completo en un único nodo de IBM Spectrum Protect o de partes del clúster en varios nodos.


Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster

Antes de configurar IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster, registre la licencia necesaria.

Procedimiento

1. Configure la biblioteca de cintas y los medios. Consulte el apartado Configuración de una biblioteca de cintas para operaciones NDMP, donde los pasos siguientes se describen con más información.
 - a. Conecte la SCSI o la biblioteca virtual de cintas (VTL) al servidor de archivos de NAS o al servidor de IBM Spectrum Protect, o conecte la biblioteca ACSLS o la biblioteca 349X al servidor de IBM Spectrum Protect.
 - b. Defina la biblioteca con un tipo de biblioteca SCSI, VTL, ACSLS o 349X.
 - c. Defina una clase de dispositivo para unidades de cintas.
 - d. Defina una agrupación de almacenamiento para medios de copia de seguridad NAS.
 - e. Opcional: Defina una agrupación de almacenamiento para almacenar una tabla de contenido.
2. Configure la política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Consulte el apartado Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
3. Registre un nodo de servidor de archivos NAS con el servidor de IBM Spectrum Protect. Consulte el apartado Registro de nodos NAS con el servidor de IBM Spectrum Protect.
4. Defina un transportador de datos para el servidor de archivos NAS. Consulte el apartado Definición de un transportador de datos para un servidor de archivos de NAS.
5. Defina una vía de acceso desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS a la biblioteca. Consulte el apartado Definición de vías de acceso a bibliotecas para operaciones NDMP.
6. Defina las unidades de cintas en IBM Spectrum Protect y defina las vías de acceso a dichas unidades desde el servidor de archivos NAS y, opcionalmente, desde el servidor de IBM Spectrum Protect. Consulte el apartado Definición de vías de acceso para operaciones NDMP.
7. Dé de alta las cintas en la biblioteca y etiquételas.

 Sistemas operativos AIX  Sistemas operativos Linux Los volúmenes de cinta deben estar etiquetados antes de que el servidor pueda utilizarlos. Puede utilizar el mandato LABEL LIBVOLUME, o puede utilizar el parámetro AUTOLABEL con los mandatos DEFINE LIBRARY y UPDATE LIBRARY.

 Sistemas operativos Windows Todos los medios deben estar etiquetados. El etiquetado de medios con una biblioteca automatizada requiere que los medios se den de alta en la biblioteca. Para etiquetar volúmenes con el mandato LABEL LIBVOLUME, especifique el parámetro CHECKIN. Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los mandatos DEFINE LIBRARY y UPDATE LIBRARY.

Para obtener instrucciones, consulte LABEL LIBVOLUME, DEFINE LIBRARY y UPDATE LIBRARY.

8. Opcional: Configure las copias de seguridad planificadas para servidores de archivos NAS. Consulte el apartado Planificación de operaciones NDMP.
 9. Opcional: Defina un nombre del espacio de archivos virtual. Consulte el apartado Definición de espacios de archivos virtuales.
 10. Opcional: Configure la copia de cinta a cinta para que realice la copia de seguridad de los datos. Consulte el apartado Copia de seguridad de datos mediante la función de cinta a cinta.
 11. Opcional: Configure la copia de cinta a cinta para que traspase los datos a otra tecnología de cinta. Consulte el apartado Traslado de datos con la función de copia de cinta a cinta.
- Configuración de una política de IBM Spectrum Protect para operaciones NDMP
Con las políticas, puede gestionar el número y el período de retención de versiones de copia de seguridad de imágenes NDMP.
 - Bibliotecas y unidades de cintas para operaciones NDMP
La mayor parte de la planificación necesaria para implementar operaciones de copia de seguridad y recuperación que utilizan NDMP está relacionada con la configuración de los dispositivos. Puede elegir cómo conectar las bibliotecas y las unidades.
 - Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS
Si tiene previsto realizar una copia de seguridad de datos de NAS en una biblioteca directamente conectada al dispositivo NAS y utilizar una biblioteca de cintas SCSI, debe determinar dónde se debe conectar la biblioteca.
 - Registro de nodos NAS con el servidor de IBM Spectrum Protect
Registre el servidor de archivos NAS como nodo de IBM Spectrum Protect, especificando TYPE=NAS. Este nombre de nodo sirve para realizar un seguimiento de las copias de seguridad de imagen para el servidor de archivos NAS.
 - Definición de un transportador de datos para un servidor de archivos de NAS
Defina un transportador de datos para cada servidor de archivos NAS utilizando las operaciones NDMP en el entorno. El nombre del transportador de datos debe coincidir con el nombre de nodo especificado al inscribir el nodo NAS en el servidor de IBM Spectrum Protect.
 - Definición de vías de acceso para operaciones NDMP
Para operaciones NDMP, se crean vías de acceso a unidades y a bibliotecas.
 - Planificación de operaciones NDMP
Puede programar operaciones de copia de seguridad o restauración de las imágenes generadas por las operaciones NDMP. Utilice las planificaciones de administración que procesan los mandatos de administración BACKUP NODE o RESTORE NODE.
 - Definición de espacios de archivos virtuales
Utilice una definición de espacio de archivos virtual para realizar copias de seguridad a nivel de directorios NAS. Para reducir el tiempo de copia de seguridad y restauración para sistemas de archivos grandes, correlacione una vía de acceso de directorios desde un servidor de archivos de NAS a un nombre del espacio de archivos virtual en el servidor de IBM Spectrum Protect.

- Copia de seguridad de datos mediante la función de cinta a cinta
Cuando utilice la función de cinta a cinta de NDMP para realizar la copia de seguridad de los datos, el tipo de biblioteca puede ser SCSI, 349X o ACSLS (software de biblioteca del sistema de cartuchos automatizados). Las unidades se pueden compartir entre los dispositivos NAS y el servidor de IBM Spectrum Protect.
- Traslado de datos con la función de copia de cinta a cinta
Para traspasar datos de una tecnología de cinta antigua a otra nueva mediante la operación de copia de cinta a cinta de NDMP, debe realizar los pasos de configuración habituales, así como otros adicionales.

Configuración de una política de IBM Spectrum Protect para operaciones NDMP

Con las políticas, puede gestionar el número y el período de retención de versiones de copia de seguridad de imágenes NDMP.

Acerca de esta tarea

Para obtener más información, consulte el apartado Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect.

Procedimiento

Complete los pasos siguientes para configurar una política para operaciones NDMP:

1. Cree un dominio de políticas para servidores de archivos NAS (almacenamiento adjunto de red). Por ejemplo, para definir un dominio de políticas con el nombre NASDOMAIN, especifique el mandato siguiente:

```
define domain nasdomain description='Dominio de políticas para servidores de
archivos NAS'
```

2. Cree un juego de políticas en ese dominio. Por ejemplo, para definir un conjunto de políticas denominado STANDARD en el dominio de políticas denominado NASDOMAIN, emita el siguiente mandato:

```
define policyset nasdomain standard
```

3. Defina una clase de gestión y, a continuación, asígnela como clase de gestión predeterminada para el juego de políticas. Por ejemplo, para definir una clase de gestión denominada MC1 en el conjunto de políticas STANDARD y asignarla como clase predeterminada, especifique los mandatos siguientes:

```
define mgmtclass nasdomain standard mc1
assign defmgmtclass nasdomain standard mc1
```

4. Defina un grupo de copia de seguridad en la clase de gestión predeterminada. El destino debe ser la agrupación de almacenamiento creada para las imágenes de copia de seguridad generadas por las operaciones NDMP. Asimismo, puede especificar el número de versiones de copia de seguridad que se deben retener. Por ejemplo, para definir un grupo de copia de seguridad para la clase de gestión MC1, en la que se retienen hasta cuatro versiones de cada sistema de archivos en la agrupación de almacenamiento NASPOOL, emita el mandato siguiente:

```
define copygroup nasdomain standard mc1 destination=naspool verexists=4
```

Si desea crear una tabla de contenido para las copias de seguridad, el parámetro TOCDESTINATION del grupo de copias debe contener el nombre de la agrupación de almacenamiento primario.

```
define copygroup nasdomain standard mc1 destination=naspool
tocdestination=tocpool verexists=4
```

Importante: Cuando define un grupo de copias para una clase de gestión en el que se encontrará una imagen de sistema de archivos producida por NDMP, asegúrese de que el parámetro DESTINATION especifique el nombre de una agrupación de almacenamiento que se haya definido para las operaciones NDMP. Si el parámetro DESTINATION especifica una agrupación de almacenamiento no válida, las copias de seguridad realizadas mediante NDMP fallan.

5. Active el juego de políticas. Por ejemplo, para activar el juego de políticas STANDARD en el dominio de políticas NASDOMAIN, emita el siguiente mandato:

```
activate policyset nasdomain standard
```

El juego de políticas está listo para utilizarlo. Los nodos se asocian a una política cuando se registran. Para obtener más información, consulte el apartado Registro de nodos NAS con el servidor de IBM Spectrum Protect.

- Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect
Puede registrar un servidor de archivos NAS (almacenamiento adjunto de red) como un nodo utilizando operaciones NDMP (Protocolo de gestión de datos de redes). Con el control del servidor de IBM Spectrum Protect, el servidor de archivos NAS realiza copias de seguridad y restaura imágenes de sistemas de archivos y de directorios en una biblioteca de cintas.
- Políticas para copias de seguridad iniciadas con la interfaz de cliente
Cuando un cliente inicia una copia de seguridad, el archivo de opciones de ese nodo de cliente influye en la política.
- Determinación de la ubicación de copia de seguridad NAS
Cuando IBM Spectrum Protect utiliza NDMP para proteger servidores de archivos NAS, el servidor de IBM Spectrum Protect controla las operaciones. Durante este tiempo, el servidor de archivos NAS transfiere los datos a una biblioteca conectada o directamente al servidor de IBM Spectrum Protect.

Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect

Puede registrar un servidor de archivos NAS (almacenamiento adjunto de red) como un nodo utilizando operaciones NDMP (Protocolo de gestión de datos de redes). Con el control del servidor de IBM Spectrum Protect, el servidor de archivos NAS realiza copias de seguridad y restaura imágenes de sistemas de archivos y de directorios en una biblioteca de cintas.

El servidor de IBM Spectrum Protect inicia la copia de seguridad, asigna una unidad y selecciona y monta los medios. A continuación, el servidor de archivos NAS transfiere los datos a la cinta.

Puesto que el servidor de archivos NAS realiza una copia de seguridad de los datos, estos se almacenan en su propio formato. Para la mayoría de los servidores NAS, los datos se almacenan en formato de datos NDMPDUMP. En los servidores de archivos NetApp, los datos se almacenan en el formato de datos NETAPPDUMP. En el caso de los servidores de archivos EMC, los datos se almacenan con el formato de datos CELERRADUMP. Para gestionar copias de seguridad de imagen del servidor de archivos NAS; los grupos de copia para los nodos NAS deben hacer referencia a una agrupación de almacenamiento que tenga un formato de datos NDMPDUMP, NETAPPDUMP o CELERRADUMP.

Los siguientes atributos de grupo de copia de seguridad se pasan por alto para imágenes NAS:

- Frecuencia
- Modalidad
- Retener única versión
- Serialización
- Versiones si datos suprimidos

Para configurar la política necesaria para los nodos NAS, puede definir un dominio de políticas nuevo y separado.

Cuando el servidor de IBM Spectrum Protect crea una tabla de contenido, puede ver un conjunto de archivos y directorios individuales cuya copia de seguridad se ha realizado mediante NDMP. A continuación, puede seleccionar los archivos y directorios que desea restaurar. Para establecer adónde se enviarán los datos y almacenar la tabla de contenidos, establezca la política de la forma siguiente:

- Asegúrese de que los datos de copia de seguridad de imagen se envían a una agrupación de almacenamiento con un formato NDMPDUMP, NETAPPDUMP o CELERRADUMP.
- Asegúrese de que la tabla de contenidos se envíe a una agrupación de almacenamiento con el formato NATIVE o NONBLOCK.

Políticas para copias de seguridad iniciadas con la interfaz de cliente

Cuando un cliente inicia una copia de seguridad, el archivo de opciones de ese nodo de cliente influye en la política.

Puede controlar las clases de gestión que se aplican a las imágenes de copia de seguridad generadas por las operaciones NDMP (Protocolo de gestión de datos de redes) independientemente del nodo que inicia la copia de seguridad. Puede completar esta tarea creando un conjunto de opciones para que lo utilicen los nodos cliente. El conjunto de opciones puede incluir una sentencia `include.fs.nas` para especificar la clase de gestión para las copias de seguridad del servidor de archivos NAS (almacenamiento adjunto de red).

Consejo: Puede definir un conjunto de opciones utilizando el mandato DEFINE CLOPTSET. A continuación, añada una opción de cliente al conjunto de opciones utilizando el mandato DEFINE CLIENTOPT. Puede asignar un conjunto de opciones a un cliente completando los pasos siguientes:

1. Abra la página Descripción general del Centro de operaciones y haga clic en Clientes.
2. Efectúe una doble pulsación en el cliente y haga clic en Propiedades.
3. En el campo Conjunto de opciones, seleccione un conjunto de opciones y haga clic en Guardar.

Para obtener instrucciones sobre cómo utilizar el mandato DEFINE CLOPTSET, consulte DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente). Para obtener instrucciones sobre cómo utilizar el mandato DEFINE CLIENTOPT, consulte DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones).

Determinación de la ubicación de copia de seguridad NAS

Cuando IBM Spectrum Protect utiliza NDMP para proteger servidores de archivos NAS, el servidor de IBM Spectrum Protect controla las operaciones. Durante este tiempo, el servidor de archivos NAS transfiere los datos a una biblioteca conectada o directamente al servidor de IBM Spectrum Protect.

También puede utilizar un cliente de copia de seguridad/archivado para realizar la copia de seguridad de un servidor de archivos NAS montando el sistema de archivos NAS en la máquina cliente y realizando la copia de seguridad de la forma usual. Puede utilizar un montaje de sistema de archivos de red (NFS) o una correlación de sistema de archivos de Internet común (CIFS).

Para obtener una descripción de los métodos de copia de seguridad y restauración, consulte Tabla 1.

Consejo: Puede utilizar un único método o una combinación de métodos en su entorno de almacenamiento individual.

Tabla 1. Comparación de métodos de copia de seguridad de los datos NDMP

Propiedad	NDMP: de servidor de archivos a servidor	NDMP: de servidor de archivos a biblioteca conectada	De cliente de copia de seguridad/archivado a servidor
Tráfico de datos en la red	Todos los datos de la copia de seguridad se desplazan por la LAN desde el servidor de archivos NAS hasta el servidor.	El servidor controla remotamente las operaciones, aunque el dispositivo NAS traspasa los datos de forma local.	Todos los datos de copia de seguridad se desplazan por la LAN desde el dispositivo NAS hasta el cliente y desde éste hasta el servidor.
Proceso del servidor de archivos durante la copia de seguridad	Se precisan menos procesos de servidor de archivos, en comparación con el método de cliente de copia de seguridad/archivado, ya que la copia de seguridad no utiliza protocolos de acceso a archivos, como NFS y CIFS.	Se precisan menos procesos de servidor de archivos, en comparación con el método de cliente de copia de seguridad/archivado, ya que la copia de seguridad no utiliza protocolos de acceso a archivos, como NFS y CIFS.	Las operaciones de copia de seguridad de archivos requieren más recursos de proceso de servidor para protocolos de acceso a archivos, como NFS y CIFS.
Distancia entre dispositivos	El servidor de IBM Spectrum Protect debe encontrarse dentro del rango del canal de fibra o SCSI de la biblioteca de cintas.	El servidor de IBM Spectrum Protect puede estar alejado del servidor de archivos NAS y de la biblioteca de cintas.	El servidor de IBM Spectrum Protect debe encontrarse dentro del rango del canal de fibra o SCSI de la biblioteca de cintas.
Consideraciones acerca del cortafuegos	Más estricto que el método de archivador a biblioteca conectada porque las comunicaciones las puede iniciar el servidor de IBM Spectrum Protect o el servidor de archivos NAS.	Menos estricto que el método de archivador a servidor ya que sólo el servidor de IBM Spectrum Protect puede iniciar las comunicaciones.	Los datos y las contraseñas de cliente están cifradas.
Consideraciones de seguridad	Los datos se envían descifrados desde un servidor de archivos NAS a un servidor de IBM Spectrum Protect.	El método debe utilizarse en un entorno de confianza porque los números de puerto no son seguros.	La configuración del número de puerto permite efectuar sesiones de administración seguras en una red privada.
Carga en el servidor de IBM Spectrum Protect	Se necesita una carga de trabajo de CPU superior para gestionar todos los procesos de datos back-end (por ejemplo, migración).	La carga de trabajo de CPU se reduce porque ya no se admiten ni la migración ni la reclamación.	Se necesita una carga de trabajo de CPU superior para gestionar todos los procesos de datos back-end.

Propiedad	NDMP: de servidor de archivos a servidor	NDMP: de servidor de archivos a biblioteca conectada	De cliente de copia de seguridad/archivado a servidor
Copia de seguridad de las agrupaciones de almacenamiento primarias en las agrupaciones de almacenamiento de copia	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el formato de datos NATIVE.	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el mismo formato de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP).	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el formato de datos NATIVE.
Restauración de agrupaciones de almacenamiento primarias y volúmenes desde agrupaciones de almacenamiento de copia	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el formato de datos NATIVE.	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el mismo formato NDMP.	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el formato de datos NATIVE.
Traspaso de datos NDMP desde volúmenes de agrupaciones de almacenamiento	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene un formato de datos NATIVE.	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene el mismo formato de datos NDMP.	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene un formato de datos NATIVE.
Migración de una agrupación de almacenamiento primaria a otra	Permitido	No permitido	Permitido
Reclamación de una agrupación de almacenamiento	Permitido	No permitido	Permitido
Operaciones de grabación simultánea durante las copias de seguridad	No permitido	No permitido	Permitido
Operaciones de exportación e importación	No permitido	No permitido	Permitido
Generación de juegos de copias de seguridad	No permitido	No permitido	Permitido
Comprobación de redundancia cíclica (CRC) cuando los datos se traspasan empleando procesos de IBM Spectrum Protect	Permitido	No permitido	Permitido
Validación mediante mandatos de auditoría de IBM Spectrum Protect	Permitido	No permitido	Permitido
Gestor de recuperación ante siniestro	Permitido	Permitido	Permitido

Bibliotecas y unidades de cintas para operaciones NDMP

La mayor parte de la planificación necesaria para implementar operaciones de copia de seguridad y recuperación que utilizan NDMP está relacionada con la configuración de los dispositivos. Puede elegir cómo conectar las bibliotecas y las unidades.

Muchas de las opciones de configuración para bibliotecas y unidades se determinan mediante las funciones de hardware de las bibliotecas. Puede configurar operaciones NDMP con bibliotecas y unidades no admitidas. Sin embargo, cuantas más funciones tenga la biblioteca, mayor será la flexibilidad de que dispondrá la implementación.

Puede empezar respondiendo a las preguntas siguientes:

- ¿Qué tipo de biblioteca (SCSI, ACSLS o 349X) utilizará?
- Si utiliza una biblioteca SCSI, ¿desea conectar robots de biblioteca de cintas al servidor de IBM Spectrum Protect o al servidor de archivos NAS (almacenamiento adjunto de red)?
- ¿Deseará trasladar los datos NDMP a cinta?
- ¿Cómo desea utilizar las unidades de cintas en la biblioteca?
 - Dedicará todas las unidades de cintas a operaciones NDMP.

- Dedicará algunas unidades de cintas a operaciones NDMP y otras unidades a operaciones tradicionales de IBM Spectrum Protect.
- Compartirá unidades de cintas entre operaciones NDMP y operaciones tradicionales de IBM Spectrum Protect.
- ¿Realizará la copia de seguridad de datos de cinta a cinta para las funciones de recuperación tras siniestro?
- ¿Enviará los datos de copia de seguridad a un único servidor de IBM Spectrum Protect en vez de conectar una biblioteca de cintas a cada dispositivo NAS?
- ¿Desea conservar todo el hardware en el servidor de IBM Spectrum Protect y enviar los datos NDMP por la LAN?
- Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS
Se pueden utilizar unidades para varios fines debido a las configuraciones flexibles permitidas por IBM Spectrum Protect. Para operaciones NDMP, el servidor de archivos NAS debe tener acceso a la unidad. El servidor de IBM Spectrum Protect también puede tener acceso a la misma unidad, en función de las conexiones y limitaciones de hardware.
- Configuración de una biblioteca de cintas para operaciones NDMP
Puede configurar una biblioteca de cintas para hacer copia de seguridad de un dispositivo de almacenamiento adjunto de red (NAS) a una cinta.

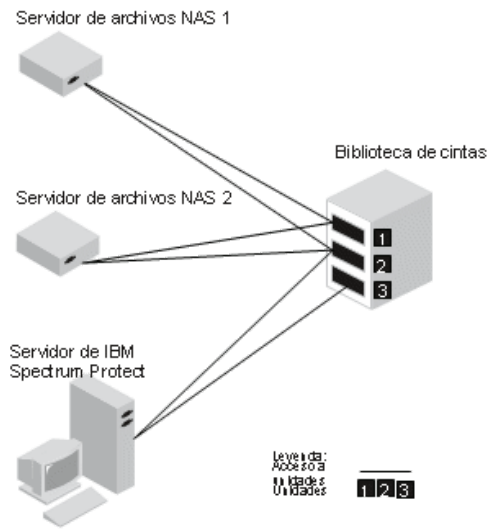
Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS

Se pueden utilizar unidades para varios fines debido a las configuraciones flexibles permitidas por IBM Spectrum Protect. Para operaciones NDMP, el servidor de archivos NAS debe tener acceso a la unidad. El servidor de IBM Spectrum Protect también puede tener acceso a la misma unidad, en función de las conexiones y limitaciones de hardware.

Acerca de esta tarea

Todas las unidades se definen en el servidor de IBM Spectrum Protect. Sin embargo, se puede definir la misma unidad para las operaciones de IBM Spectrum Protect y las operaciones de NDMP tradicionales. En la Figura 1 se muestra una posible configuración. El servidor de IBM Spectrum Protect tiene acceso a las unidades 2 y 3, y cada servidor de archivos NAS tiene acceso a las unidades 1 y 2.

Figura 1. Ejemplo de uso de la unidad de IBM Spectrum Protect



Para crear la configuración que se muestra en Figura 1, complete los pasos siguientes:

Procedimiento

1. Defina las tres unidades en IBM Spectrum Protect.

2. Defina las vías de acceso desde el servidor de IBM Spectrum Protect a las unidades 2 y 3. Puesto que el servidor no accede a la unidad 1, no se define ninguna vía de acceso.
3. Defina cada servidor de archivos NAS como transportador de datos separado.
4. Defina vías de acceso desde cada transportador de datos a las unidades 1 y 2.

Resultados

Para utilizar las operaciones de movimiento de datos de programa de fondo de IBM Spectrum Protect, el servidor de IBM Spectrum Protect necesita dos vías de acceso de unidad disponibles desde un único transportador de datos de NAS. Las unidades pueden estar en bibliotecas diferentes y tener tipos de dispositivos diferentes con soporte de NDMP. Puede realizar copias entre dos diferentes dispositivos de cinta. Por ejemplo, la unidad de cintas de origen puede ser una unidad DLT de una biblioteca y la unidad de destino puede ser una unidad LTO de otra biblioteca.

Durante los movimientos de datos de programa de fondo de IBM Spectrum Protect, el servidor de IBM Spectrum Protect localiza un transportador de datos de NAS que soporte el mismo formato de datos como el de los datos que se deben copiar y que tenga dos puntos de montaje disponibles y vías de acceso a las unidades. Si el servidor de IBM Spectrum Protect no puede localizar un transportador de datos de este tipo, la operación de traspaso de datos solicitada no se llevará a cabo. El número de puntos de montaje y unidades disponibles depende de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento que están implicadas en los movimientos de datos de programa de fondo.

Si la función de movimiento de datos de programa de fondo soporta multiproceso, cada movimiento de datos de programa de fondo de IBM Spectrum Protect simultáneo necesita dos puntos de montaje disponibles y dos unidades disponibles. Para ejecutar dos procesos de IBM Spectrum Protect simultáneamente, debe haber como mínimo cuatro puntos de montaje y cuatro unidades disponibles.

Para obtener más información, consulte Definición de vías de acceso para operaciones NDMP.

Configuración de una biblioteca de cintas para operaciones NDMP

Puede configurar una biblioteca de cintas para hacer copia de seguridad de un dispositivo de almacenamiento adjunto de red (NAS) a una cinta.

Procedimiento

Complete los siguientes pasos para configurar las bibliotecas de cintas para operaciones NDMP:

1. Conecte la biblioteca y las unidades que se van a utilizar para operaciones NDMP.
 - a. Conecte la biblioteca SCSI. Antes de configurar una biblioteca de cintas SCSI para operaciones NDMP, debe haber determinado si desea conectar el control robótico de la biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos de NAS. Consulte el apartado Bibliotecas y unidades de cintas para operaciones NDMP. Conecte el robot de la biblioteca de cintas SCSI al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Consulte la documentación del fabricante del dispositivo para obtener instrucciones.

Si la biblioteca está conectada a IBM Spectrum Protect, establezca una conexión SCSI o de canal de fibra entre el servidor de IBM Spectrum Protect y el puerto de control robótico de la biblioteca. A continuación, conecte el servidor de archivos de NAS a las unidades.

Si la biblioteca está conectada al servidor de archivos NAS, realice una conexión SCSI o de canal de fibra entre el servidor de archivos NAS y las unidades o la robótica de biblioteca.
 - b. Conecte la biblioteca ACSLS. Conecte la biblioteca de cintas ACSLS al servidor de IBM Spectrum Protect.
 - c. Conecte la biblioteca 349X. Conecte la biblioteca de cintas 349X al servidor de IBM Spectrum Protect.
2. Defina una biblioteca para los dispositivos de biblioteca emitiendo el mandato DEFINE LIBRARY. La biblioteca tiene que ser de un solo tipo de dispositivo, no de una mezcla de dispositivos. Emita uno de los mandatos siguientes para definir la biblioteca en función del tipo de dispositivo que esté configurando:

Biblioteca SCSI

```
define library tsmlib libtype=scsi
```

Biblioteca ACSLS

```
define library acslib libtype=acsls acsid=1
```

Biblioteca 349X

```
define library tsmlib libtype=349x
```

3. Defina una clase de dispositivo para el dispositivo NDMP emitiendo el mandato DEFINE DEVCLASS.

Consejo: Una clase de dispositivo que está definida con un tipo de dispositivo de NAS no está asociada explícitamente a un tipo de unidad específico, por ejemplo, LTO. Sin embargo, la práctica recomendada es definir una clase de dispositivo independiente para tipos de unidades diferentes.

En el mandato DEFINE DEVCLASS, utilice los siguientes parámetros y valores:

- o Especifique DEVTYPE=NAS.
- o Especifique MOUNTRETENTION=0. Es necesario para las operaciones NDMP.
- o Especifique un valor para el parámetro ESTCAPACITY.

Por ejemplo, para definir una clase de dispositivo denominada NASCLASS para una biblioteca denominada NASLIB con una capacidad estimada de 40 GB para el soporte, emita el siguiente mandato:

```
define devclass nasclass devtype=nas library=naslib mountretention=0
  estcapacity=40g
```

4. Defina una agrupación de almacenamiento para soportes NDMP emitiendo el mandato DEFINE STGPOOL. Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales. Las operaciones de IBM Spectrum Protect utilizan agrupaciones de almacenamiento definidas con un formato de datos NATIVE o NONBLOCK. Si selecciona NETAPPDUMP, CELERRADUMP o NDMPDUMP, las operaciones NDMP necesitarán agrupaciones de almacenamiento que dispongan de un formato de datos que coincida con el servidor de archivos de NAS y el método de copia de seguridad seleccionado. Se recomienda mantener agrupaciones de almacenamiento separadas para datos de proveedores de NAS diferentes, aunque el formato de datos de ambos sea NDMPDUMP. Por ejemplo, para definir una agrupación de almacenamiento denominada NDMPPool para un servidor de archivos que no sea un servidor de archivos Celerra o NetApp, emita el siguiente mandato:

```
define stgpool ndmppool nasclass maxscratch=10 dataformat=ndmpdump
```

Para definir una agrupación de almacenamiento denominada NASPOOL para un servidor de archivos NetApp, emita el siguiente mandato:

```
define stgpool naspool nasclass maxscratch=10 dataformat=netappdump
```

Para definir una agrupación de almacenamiento denominada CELERRAPOOL para un servidor de archivos EMC Celerra, emita el siguiente mandato:



```
define stgpool celerrapool nasclass maxscratch=10 dataformat=celerradump
```


Atención: Asegúrese de que en las operaciones tradicionales de IBM Spectrum Protect no utilizan por accidente agrupaciones de almacenamiento definidas para operaciones NDMP. Sea especialmente precavido cuando asigne al nombre de agrupación de almacenamiento el valor del parámetro DESTINATION del mandato DEFINE COPYGROUP. Si el destino no es una agrupación de almacenamiento con el formato de datos adecuado, la operación de copia de seguridad fallará.



5. Opcional: Defina una agrupación de almacenamiento para una tabla de contenido. Si tiene previsto crear una tabla de contenido, también debe definir una agrupación de almacenamiento en disco en la que almacenar la tabla de contenido. Debe configurar la política de modo que el servidor de IBM Spectrum Protect almacene la tabla de contenido en una agrupación de almacenamiento distinta de la empleada para almacenar la imagen de copia de seguridad. La tabla de contenido se maneja del mismo modo que cualquier otro objeto de esa agrupación de almacenamiento. Por ejemplo, para definir una agrupación de almacenamiento denominada TOCPool para una clase de dispositivo DISK, emita el siguiente mandato:

```
define stgpool tocpool disk
```

Posteriormente, defina volúmenes para la agrupación de almacenamiento.

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#) Para obtener más información sobre la definición de volúmenes, consulte [Configuración de volúmenes de acceso aleatorio en dispositivos de disco \(V7.1.1\)](#).

 [Sistemas operativos Windows](#) Para obtener más información sobre la definición de volúmenes, consulte [Configuración de volúmenes de acceso aleatorio en dispositivos de disco \(V7.1.1\)](#).

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#) Para obtener más información sobre la configuración de bibliotecas, consulte [Configuración de bibliotecas para su uso por parte de un servidor](#).

Referencia relacionada:

DEFINE DEVCLASS (Definir una clase de dispositivo)

Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS

Si tiene previsto realizar una copia de seguridad de datos de NAS en una biblioteca directamente conectada al dispositivo NAS y utilizar una biblioteca de cintas SCSI, debe determinar dónde se debe conectar la biblioteca.













Acerca de esta tarea

Debe determinar si conectará el robot de biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Independientemente de dónde conecte el robot de biblioteca, las unidades de cintas siempre deben estar conectadas al servidor de archivos NAS para operaciones NDMP.

Debe tener en cuenta la distancia y las conexiones de hardware disponibles para las bibliotecas SCSI. Si la biblioteca no tiene puertos separados para control robótico y acceso a las unidades, la biblioteca debe estar conectada al servidor de archivos NAS porque el servidor de archivos debe tener acceso a las unidades. Si la biblioteca SCSI tiene puertos separados para el control robótico y el acceso a las unidades, puede elegir conectar el robot de la biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos NAS indistintamente. Si el servidor de archivos NAS tiene una ubicación diferente del servidor de IBM Spectrum Protect, la distancia puede significar que debe conectar la biblioteca al servidor de archivos NAS.

Tanto si utiliza una biblioteca SCSI, ACSLS o 349X, tiene la opción de dedicar la biblioteca a las operaciones NDMP o de utilizar la biblioteca para las operaciones NDMP. También puede utilizar la biblioteca para la mayoría de las operaciones tradicionales de IBM Spectrum Protect.

Tabla 1. Resumen de configuraciones para operaciones NDMP

Configuración	Distancia entre el servidor de IBM Spectrum Protect y la biblioteca	Compartición de biblioteca	Compartición de unidades entre IBM Spectrum Protect y el servidor de archivos NAS	Compartición de unidades entre servidores de archivos NAS	Compartición de unidades entre el agente de almacenamiento y el servidor de archivos NAS
Configuración 1 (biblioteca SCSI conectada al servidor de IBM Spectrum Protect)	Con límite de conexión SCSI o de canal de fibra	Permitido	Permitido	Permitido	Permitido
Configuración 2 (biblioteca SCSI conectada al servidor NAS)	Sin límite	No permitido	Permitido	Permitido	No permitido
Configuración 3 (biblioteca 349X)	Con posible límite de conexión 349X	Permitido	Permitido	Permitido	Permitido
 Sistemas operativos AIX  Sistemas operativos Windows Configuración 4 (biblioteca ACSLS)	 Sistemas operativos AIX  Sistemas operativos Windows Con posible límite de conexión ACSLS	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido

- Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect
En esta configuración, la biblioteca de cintas debe tener puertos separados para el control robótico y para el acceso a las unidades. Además, la biblioteca debe estar al alcance del canal de fibra o del bus SCSI tanto del servidor de IBM Spectrum Protect como del servidor de archivos NAS.
- Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS
En esta configuración, el robot de la biblioteca y las unidades deben estar conectadas directamente al servidor de archivos NAS. Deben definirse vías de acceso desde el transportador de datos NAS a la biblioteca y a las unidades. No es necesaria ninguna conexión física entre el servidor de IBM Spectrum Protect y la biblioteca SCSI.
- Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect
Para esta configuración la biblioteca de cintas se conecta al sistema igual que para las operaciones tradicionales.
- Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect
Para esta configuración, conecte la biblioteca de cintas al sistema igual que para las operaciones de IBM Spectrum Protect tradicionales.

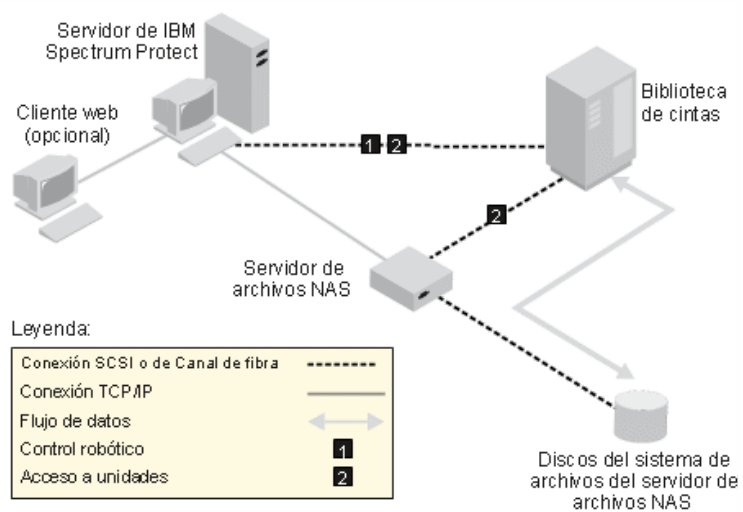
Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect

En esta configuración, la biblioteca de cintas debe tener puertos separados para el control robótico y para el acceso a las unidades. Además, la biblioteca debe estar al alcance del canal de fibra o del bus SCSI tanto del servidor de IBM Spectrum Protect como del servidor de archivos NAS.

En esta configuración, el servidor de IBM Spectrum Protect controla la biblioteca SCSI mediante una conexión física directa al puerto de control robótico de la biblioteca. Para operaciones NDMP, las unidades de la biblioteca están conectadas directamente al servidor de archivo NAS, y se debe definir la vía de acceso desde el transportador de datos NAS hasta cada una de las unidades que se van a utilizar. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Para utilizar también las unidades para operaciones de IBM Spectrum Protect, conecte el servidor de IBM Spectrum Protect a las unidades de cintas y defina las vías de acceso desde el servidor hasta las unidades de cintas.

Esta configuración también admite un agente de almacenamiento de IBM Spectrum Protect con acceso a las unidades para sus operaciones fuera de la LAN, y el servidor de IBM Spectrum Protect puede ser un gestor de biblioteca.

Figura 1. Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect



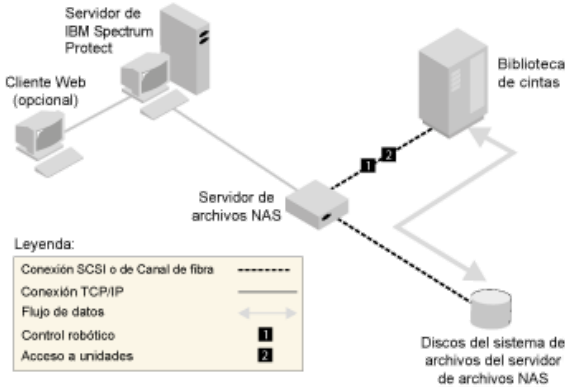
Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS

En esta configuración, el robot de la biblioteca y las unidades deben estar conectadas directamente al servidor de archivos NAS. Deben definirse vías de acceso desde el transportador de datos NAS a la biblioteca y a las unidades. No es necesaria ninguna conexión física

entre el servidor de IBM Spectrum Protect y la biblioteca SCSI.

El servidor de IBM Spectrum Protect controla el robot de la biblioteca enviando mandatos de biblioteca al servidor de archivos NAS a través de la red. El servidor de archivos NAS pasa los mandatos a la biblioteca de cintas. Las respuestas que genera la biblioteca se envían al servidor de archivos NAS y se devuelven al servidor de IBM Spectrum Protect a través de la red. Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect está en una ciudad y el servidor de archivos NAS y la biblioteca de cintas está en otra ciudad.

Figura 1. Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS



Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect

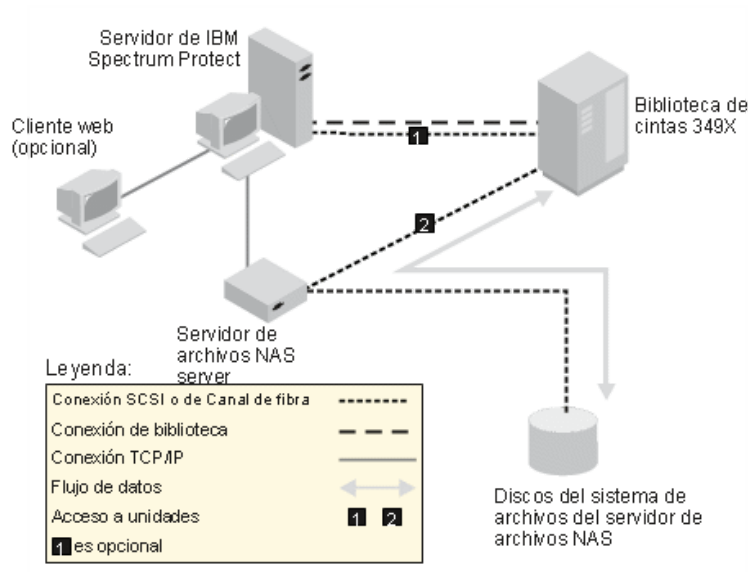
Para esta configuración la biblioteca de cintas se conecta al sistema igual que para las operaciones tradicionales.

En esta configuración, el servidor de IBM Spectrum Protect controla la biblioteca de cintas 349X. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud al gestor de la biblioteca 349X a través de TCP/IP.

Para completar las operaciones de copia de seguridad o restauración NAS (almacenamiento adjunto de red), el servidor de archivos NAS debe poder acceder a una o varias unidades de cintas de la biblioteca 349X. Todas las unidades de cintas empleadas para las operaciones NAS deben estar conectadas físicamente al servidor de archivos NAS, y deben definirse vías de acceso desde el transportador de datos NAS hasta las unidades. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Siga las instrucciones del fabricante para conectar el dispositivo al sistema servidor.

Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect puede estar en una ciudad y el servidor de archivos NAS y la biblioteca de cintas puede estar en otra.

Figura 1. Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect




Información relacionada:

[Conexión de dispositivos para el servidor](#)

Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect

Para esta configuración, conecte la biblioteca de cintas al sistema igual que para las operaciones de IBM Spectrum Protect tradicionales.

El servidor de IBM Spectrum Protect controla la biblioteca de cintas ACSLS (software de biblioteca del sistema de cartuchos automatizado). El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud al servidor de la biblioteca ACSLS a través de TCP/IP. La biblioteca ACSLS permite operaciones de compartir bibliotecas y trabajos fuera de la LAN.

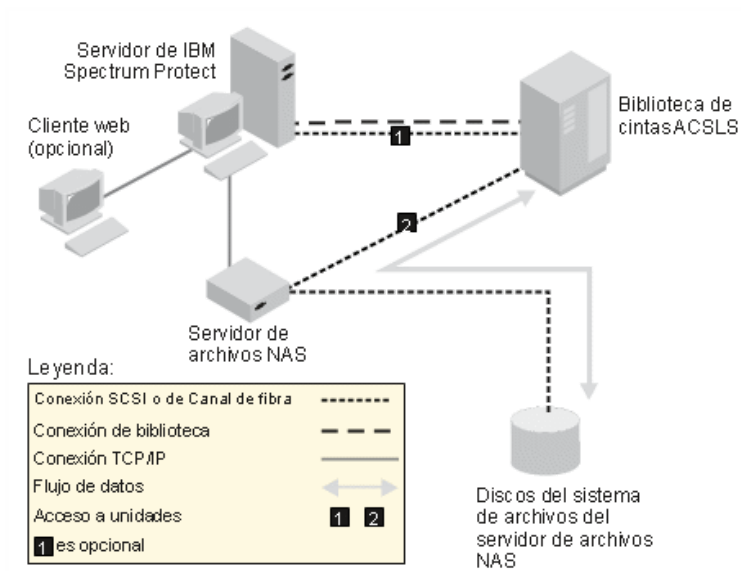
 **Sistemas operativos Windows** Restricción: Para utilizar las funciones ACSLS, debe instalarse el software StorageTek Library Attach. Para obtener más información, consulte Bibliotecas gestionadas mediante ACSLS (V7.1.1).

Para completar las operaciones de copia de seguridad o restauración NAS (almacenamiento adjunto de red), el servidor de archivos NAS debe poder acceder a una o varias unidades de cintas de la biblioteca ACSLS. Todas las unidades de cintas empleadas para las operaciones NAS deben estar conectadas físicamente al servidor de archivos NAS y deben definirse vías de acceso desde el transportador de datos NAS hasta las unidades. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Siga las instrucciones del fabricante para conectar el dispositivo al sistema servidor.

Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect puede estar en una ciudad y el servidor de archivos NAS y la biblioteca de cintas pueden estar en otra ciudad.

Para utilizar también las unidades para operaciones de IBM Spectrum Protect, conecte el servidor de IBM Spectrum Protect a las unidades de cintas y defina las vías de acceso desde el servidor de IBM Spectrum Protect hasta las unidades de cintas.

Figura 1. Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect



Información relacionada:

➔ [Conexión de dispositivos para el servidor](#)

Registro de nodos NAS con el servidor de IBM Spectrum Protect

Registre el servidor de archivos NAS como nodo de IBM Spectrum Protect, especificando TYPE=NAS. Este nombre de nodo sirve para realizar un seguimiento de las copias de seguridad de imagen para el servidor de archivos NAS.

Procedimiento

Para registrar un sistema de archivos NAS como un nodo denominado NASNODE1, con la contraseña NASPWD1, en un dominio de políticas denominado NASDOMAIN, emita el siguiente mandato de ejemplo:

```
register node nasnode1 naspwd1 domain=nasdomain type=nas
```

Si utiliza un conjunto de opciones de cliente, especifique el conjunto de opciones cuando inscriba el nodo. Puede comprobar que este nodo esté registrado emitiendo el siguiente mandato:

```
query node type=nas
```

Recuerde: Debe especificar TYPE=NAS para que sólo se visualicen los nodos de NAS.

Definición de un transportador de datos para un servidor de archivos de NAS

Defina un transportador de datos para cada servidor de archivos NAS utilizando las operaciones NDMP en el entorno. El nombre del transportador de datos debe coincidir con el nombre de nodo especificado al inscribir el nodo NAS en el servidor de IBM Spectrum Protect.

Acerca de esta tarea

IBM Spectrum Protect admite dos tipos de transportadores de datos:

- Para operaciones NDMP, los transportadores de datos son servidores de archivos NAS. La definición de un transportador de datos de NAS contiene la dirección de red, la autorización y los formatos de datos necesarios para las operaciones NDMP. Un transportador de datos permite la comunicación y garantiza la autorización para operaciones NDMP entre el servidor de IBM Spectrum Protect y el servidor de archivos NAS.
- Para el traspaso de datos fuera del servidor, los transportadores de datos son dispositivos, como por ejemplo IBM® SAN Data Gateway, que traspasa datos entre dispositivos de disco y de cintas en la SAN.

Procedimiento

Para definir un transportador de datos, utilice el mandato DEFINE DATAMOVER.

Ejemplo

Por ejemplo, defina un transportador de datos con estos parámetros:

- El nodo NAS se llama NASNODE1.
- La dirección de alto nivel es una dirección IP del servidor de archivos NAS y puede ser una dirección numérica o un nombre de host.
- La dirección de bajo nivel es el puerto IP de las sesiones NDMP con el servidor de archivos NAS. El valor predeterminado es el número de puerto 10000.
- El ID de usuario es el ID definido en el servidor de archivos NAS que autoriza una sesión de NDMP con el servidor de archivos NAS. Para este ejemplo, el ID de usuario es el ID administrativo para el servidor de archivos NetApp.
- El parámetro de contraseña es una contraseña válida para la autenticación en una sesión NDMP con el servidor de archivos NAS.
- El formato de datos es NETAPPDUMP. Este es el formato de datos que utiliza el servidor de archivos NetApp para realizar copia de seguridad de cinta. Este formato de datos debe coincidir con el formato de datos de la agrupación de almacenamiento de destino.

Entre el mandato siguiente:

```
define datamover nasnode1 type=nas haddress=netapp2 lladdress=10000 userid=root  
password=admin dataformat=netappdump
```

Referencia relacionada:

DEFINE DATAMOVER (Definir un transportador de datos)

Definición de vías de acceso para operaciones NDMP

Para operaciones NDMP, se crean vías de acceso a unidades y a bibliotecas.

- Definición de vías de acceso a unidades para operaciones NDMP
El método elegido para la creación de vías de acceso a unidades depende de si a las unidades accede un servidor de archivos NAS y el servidor de IBM Spectrum Protect, o solo un servidor de archivos NAS.
- Definición de vías de acceso a bibliotecas para operaciones NDMP
Defina una vía de acceso a la biblioteca SCSI desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS.

Definición de vías de acceso a unidades para operaciones NDMP

El método elegido para la creación de vías de acceso a unidades depende de si a las unidades accede un servidor de archivos NAS y el servidor de IBM Spectrum Protect, o solo un servidor de archivos NAS.

- Definición de vías de acceso a unidades conectadas a un servidor de archivos NAS y al servidor de IBM Spectrum Protect
Si un servidor de archivos de almacenamiento adjunto de red (NAS) y el servidor IBM Spectrum Protect deben acceder a una unidad de cintas server, debe crear dos vías de acceso. Existe una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Existe otra vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect.
- Definición de vías de acceso a unidades conectadas únicamente a servidores de archivos NAS
Si solo debe acceder a una unidad de cintas un servidor de archivos NAS y no el servidor IBM Spectrum Protect, solo es necesaria una única vía de acceso entre la unidad de cintas y el servidor de archivos NAS.
- Obtención de nombres para dispositivos conectados a servidores de archivos NAS
Para vías de acceso procedentes de un transportador de datos NAS, el valor del parámetro DEVICE en el mandato DEFINE PATH es el nombre por el cual el servidor de archivos NAS identifica la biblioteca o la unidad.

Definición de vías de acceso a unidades conectadas a un servidor de archivos NAS y al servidor de IBM Spectrum Protect

Si un servidor de archivos de almacenamiento adjunto de red (NAS) y el servidor IBM Spectrum Protect deben acceder a una unidad de cintas server, debe crear dos vías de acceso. Existe una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Existe otra vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect.

Procedimiento

Realice los pasos siguientes:

1. Si la unidad no está definida para el servidor de IBM Spectrum Protect, cree la definición de unidad. Por ejemplo, para definir una unidad NASDRIVE1 para una biblioteca NASLIB, emita el siguiente mandato:


```
define drive naslib nasdrive1 element=autodetect
```

Recuerde: Si la unidad está conectada al servidor de IBM Spectrum Protect, la dirección de elemento se detecta automáticamente.

2. Correlacione el nombre del dispositivo NAS con la definición de la unidad correspondiente en el servidor de IBM Spectrum Protect:
 - En el servidor IBM Spectrum Protect, emita el mandato QUERY DRIVE FORMAT=DETAILED para obtener el nombre de ámbito mundial (WWN) y el número de serie para la unidad que estará conectada al servidor de archivos NAS.
 - En el dispositivo NAS, obtenga el nombre del dispositivo de cinta, el número de serie y el WWN para la unidad.Si coincide el WWN o el número de serie, una unidad de un servidor de archivos NAS es la misma que la unidad del servidor de IBM Spectrum Protect.
3. Utilizando el nombre del dispositivo, defina una vía de acceso a la unidad desde el servidor de archivos NAS y una vía de acceso a la unidad desde el servidor de IBM Spectrum Protect.
 - Por ejemplo, para definir una vía de acceso entre una unidad de cintas con el nombre de dispositivo rst01 y un servidor de archivos NetApp, emita el siguiente mandato:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive  
library=naslib device=rst01
```

- Para definir una vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect, emita el mandato siguiente:

 Sistemas operativos AIX

```
define path server1 nasdrive1 srctype=server desttype=drive  
library=naslib device=/dev/rmt0
```

Sistemas operativos Linux

```
define path server1 nasdrive1 srctype=server desttype=drive
library=naslib device=/dev/tsm SCSI/mt0
```

Sistemas operativos Windows

```
define path server1 nasdrive1 srctype=server desttype=drive
library=naslib device=mt3.0.0.2
```

Definición de vías de acceso a unidades conectadas únicamente a servidores de archivos NAS

Si solo debe acceder a una unidad de cintas un servidor de archivos NAS y no el servidor IBM Spectrum Protect, solo es necesaria una única vía de acceso entre la unidad de cintas y el servidor de archivos NAS.




Procedimiento

Realice los pasos siguientes:

1. Obtenga las direcciones de elementos SCSI, los nombres de ámbito mundial (WWN) y los números de serie para la unidad que se va a conectar al servidor de archivos NAS.

Restricción: Si la unidad SCSI está conectada únicamente a un servidor de archivos NAS, la dirección del elemento no se detecta automáticamente y se debe proporcionar. Si una biblioteca tiene más de una unidad, se debe especificar una dirección de elemento para cada unidad.

Para obtener una dirección de elemento SCSI, vaya a los siguientes sitios web de soporte de dispositivo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

La asignación del número de elemento y las asignaciones de los WWN de dispositivo también están disponibles en los fabricantes de dispositivos de biblioteca de cintas.

2. Cree definiciones de unidades especificando las direcciones de elemento identificadas en el paso precedente. Especifique la dirección de elemento en el parámetro ELEMENT del mandato DEFINE DRIVE. Por ejemplo, para definir una unidad NASDRIVE1 con la dirección de elemento 82 para la biblioteca NASLIB, emita el siguiente mandato:

```
define drive naslib nasdrive1 element=82
```

Atención: Para una unidad conectada sólo al servidor de archivos NAS, no especifique ASNEEDED como valor para el parámetro CLEANFREQUENCY del mandato DEFINE DRIVE.

3. Obtenga el nombre del dispositivo, el número de serie y el WWN para la unidad en el dispositivo NAS.
4. Con la información obtenida en los pasos 1 y 3, correlacione el nombre del dispositivo de NAS con la dirección de elemento en la definición de unidad en el servidor de IBM Spectrum Protect.
5. Defina una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Por ejemplo, para definir una vía de acceso entre un servidor de archivos NetApp y una unidad de cintas con un nombre de dispositivo rst01, emita el siguiente mandato:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive
library=naslib device=rst01
```

Obtención de nombres para dispositivos conectados a servidores de archivos NAS

Para vías de acceso procedentes de un transportador de datos NAS, el valor del parámetro DEVICE en el mandato DEFINE PATH es el nombre por el cual el servidor de archivos NAS identifica la biblioteca o la unidad.

Acerca de esta tarea

Puede obtener estos nombres de dispositivo, también denominados *nombres de archivo especial*, realizando una consulta al servidor de archivos NAS. Para obtener más información sobre cómo obtener nombres para dispositivos conectados al servidor de archivos NAS, consulte la información de producto del servidor de archivos.

Procedimiento

- Para obtener los nombres de dispositivo para bibliotecas de cintas en un servidor de archivos NetApp Release ONTAP 10.0 GX, o posterior, conéctese con el servidor de archivos mediante telnet y emita el mandato SYSTEM HARDWARE TAPE LIBRARY SHOW. Para obtener los nombres de dispositivo para unidades de cintas en un servidor de archivos NetApp Release ONTAP 10.0 GX, o

posterior, conéctese con el servidor de archivos mediante telnet y emita el mandato SYSTEM HARDWARE TAPE DRIVE SHOW. Para obtener más detalles sobre estos mandatos, consulte la documentación de producto del servidor de archivos NetApp ONTAP GX.

- Para los releases anteriores a NetApp Release ONTAP 10.0 GX, continúe utilizando el mandato SYSCONFIG. Por ejemplo, para visualizar los nombres de dispositivo para bibliotecas de cintas, conéctese al servidor de archivos mediante telnet y emita el siguiente mandato:

```
sysconfig -m
```

Para visualizar los nombres de dispositivo para unidades de cintas, emita el siguiente mandato:

```
sysconfig -t
```

- Para las unidades conectadas a canal de fibra y el transportador de datos Celerra, realice los pasos siguientes:
 1. Inicie sesión en la estación de trabajo de control de EMC Celerra utilizando un ID de administración. Emita el mandato siguiente:

```
server_devconfig server_1 -l -s -n
```

Consejo: La opción -l enumera únicamente la información de dispositivo que se ha guardado en la base de datos del transportador de datos. El mandato y la opción no muestran los cambios en la configuración del dispositivo que se han producido después de la última actualización de la base de datos en el transportador de datos. Para obtener más detalles sobre cómo obtener la configuración más reciente del dispositivo para su transportador de datos, consulte la documentación de EMC Celerra.

La salida del mandato server_devconfig incluye los nombres de dispositivo para los dispositivos conectados al transportador de datos. Los nombres de dispositivo se enumeran en la columna *addr*, por ejemplo:

```
server_1:
Scsi Device Table
name      addr      type      info
tape1     c64t010  tape     IBM ULT3580-TD2 53Y2
ttape1    c96t010  tape     IBM ULT3580-TD2 53Y2
```

2. Correlacione el nombre del dispositivo Celerra con el nombre de ámbito mundial del dispositivo (WWN):
 - a. Para mostrar el WWN, inicie sesión en la estación de trabajo de control de EMC Celerra y emita el siguiente mandato. Recuerde incluir un punto (.) as the first character in this command.

```
.server_config server_# -v "fcp bind show"
```

La salida de este mandato incluye el WWN, por ejemplo:

```
Chain 0064: WWN 500507630f418e29 HBA 2 N_PORT Bound
Chain 0096: WWN 500507630f418e18 HBA 2 N_PORT Bound
```

Consejo: El mandato .server_config es un mandato no documentado de EMC Celerra. Para obtener más información sobre cómo utilizarlo, póngase en contacto con EMC.

- b. Utilice el número de cadena para identificar el dispositivo de cinta que se mostraba en la salida del mandato server_devconfig y que tiene el mismo WWN, por ejemplo:

Nombre del dispositivo de cintas	Número de cadena	WWN
c64t010	0064	500507630f418e29
c96t010	0096	500507630f418e18

Es posible que los mandatos Celerra se comporten de forma diferente en los diferentes sistemas EMC Celerra y niveles del sistema operativo. Para conocer los detalles, consulte la documentación de EMC Celerra o póngase en contacto con EMC.

Definición de vías de acceso a bibliotecas para operaciones NDMP

Defina una vía de acceso a la biblioteca SCSI desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS.

Procedimiento

1. Para una biblioteca SCSI conectada a IBM Spectrum Protect, emita el siguiente mandato de ejemplo para definir una vía de acceso desde el servidor, denominado SERVER1, a la biblioteca SCSI denominada TSMLIB:

 Sistemas operativos AIX

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lb1
```

Sistemas operativos Linux

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/tmscsi/lb1
```

Sistemas operativos Windows

```
define path server1 tsmlib srctype=server desttype=library
device=lb0.0.0.2
```

2. Para una biblioteca SCSI conectada a un servidor de archivos NAS, emita el siguiente mandato de ejemplo para definir una vía de acceso entre un transportador de datos NetApp NAS denominado NASNODE1 y una biblioteca denominada NASLIB:

```
define path nasnode1 naslib srctype=datamover desttype=library device=mc0
```

3. Para una biblioteca 349X, defina una vía de acceso a la biblioteca desde el servidor de IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato para definir una vía de acceso del servidor, denominado SERVER1, a la biblioteca 349X denominada TSMLIB:

Sistemas operativos AIX

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lmcp0
```

Sistemas operativos Linux Sistemas operativos Windows

```
define path server1 tsmlib srctype=server desttype=library
device=library1
```

Consejo: El mandato DEFINE PATH no es necesario para una biblioteca ACSLS (software de biblioteca del sistema de cartuchos automatizados).

Planificación de operaciones NDMP

Puede programar operaciones de copia de seguridad o restauración de las imágenes generadas por las operaciones NDMP. Utilice las planificaciones de administración que procesan los mandatos de administración BACKUP NODE o RESTORE NODE.

Procedimiento


Cree una planificación utilizando el mandato DEFINE SCHEDULE. Por ejemplo, para crear una planificación de administración llamada NASSCHED para hacer una copia de seguridad de todos los sistemas de archivos para el nodo NASNODE1, especifique el siguiente mandato:

```
define schedule nassched type=administrative cmd='backup node nasnode1' active=yes
starttime=20:00 period=1 perunits=days
```

La planificación está activa y se establece para que se ejecute diariamente a las 8 de la tarde.

Restricción: Los mandatos BACKUP NODE y RESTORE NODE solo los pueden los nodos TYPE=NAS.

Tareas relacionadas:

 [Ajuste de la planificación para las operaciones diarias](#)

Referencia relacionada:

BACKUP NODE (Copia de seguridad de un nodo NAS)

RESTORE NODE (Restaurar un nodo NAS)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

Definición de espacios de archivos virtuales

Utilice una definición de espacio de archivos virtual para realizar copias de seguridad a nivel de directorios NAS. Para reducir el tiempo de copia de seguridad y restauración para sistemas de archivos grandes, correlacione una vía de acceso de directorios desde un servidor de archivos de NAS a un nombre del espacio de archivos virtual en el servidor de IBM Spectrum Protect.

Procedimiento

Para crear un nombre de espacio de archivos virtual para la vía de acceso de directorios en el dispositivo NAS, emita el mandato DEFINE VIRTUALFSMAPPING:

```
define virtualfsmapping nas1 /mikesdir /vol/vol1 /mikes
```

Este mandato define el nombre de espacio de archivos virtual /MIKESDIR en el servidor, que representa la vía de acceso de directorios /VOL/VOL1/MIKES en el servidor de archivos de NAS, representado por el nodo NAS1. Para obtener más información, consulte el apartado Copia de seguridad y restauración a nivel de directorio para operaciones NDMP.

Copia de seguridad de datos mediante la función de cinta a cinta

Cuando utilice la función de cinta a cinta de NDMP para realizar la copia de seguridad de los datos, el tipo de biblioteca puede ser SCSI, 349X o ACSLS (software de biblioteca del sistema de cartuchos automatizados). Las unidades se pueden compartir entre los dispositivos NAS y el servidor de IBM Spectrum Protect.

Acerca de esta tarea

Cuando se usa la función de copia de cinta a cinta de NDMP, la configuración puede afectar al rendimiento del movimiento de datos de back-end de IBM Spectrum Protect.

Procedimiento

Para tener un dispositivo NAS con vías de acceso a cuatro unidades en una biblioteca, utilice el mandato MOVE DATA tras completar la configuración. De esta manera, los datos del volumen VOL1 se traspasarán como VOL1 a cualquier volumen disponible de la misma agrupación de almacenamiento:

```
move data voll
```

Traslado de datos con la función de copia de cinta a cinta

Para traspasar datos de una tecnología de cinta antigua a otra nueva mediante la operación de copia de cinta a cinta de NDMP, debe realizar los pasos de configuración habituales, así como otros adicionales.

Acerca de esta tarea

Cuando se usa la función de copia de cinta a cinta de NDMP, la configuración puede afectar al rendimiento del movimiento de datos de back-end de IBM Spectrum Protect.

Procedimiento

Además de los pasos habituales de configuración, complete los siguientes pasos:

1. Defina una unidad en la biblioteca, lib1, que tenga tecnología de cinta antigua:

```
define drive lib1 drv1 element=1035
```

2. Defina una unidad de la biblioteca, lib2, que tenga tecnología de cinta nueva:

```
define drive lib2 drv1 element=1036
```

3. Defina las vías de acceso desde el servidor de archivos NAS a cada unidad:

```
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib1 device=rst11  
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib2 device=rst21
```

4. Traspase los datos del volumen vol1 de la agrupación de almacenamiento primaria a los volúmenes de otra agrupación de almacenamiento primaria, nasprimpool2:

```
move data voll stgpool=nasprimpool2
```

Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno en clúster de NetApp

Puede realizar una copia de seguridad de los datos de un clúster de NetApp en un dispositivo de cinta conectado directamente o en servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Puede realizar una copia de seguridad del clúster completo en un único nodo de IBM Spectrum Protect o de partes del clúster en varios nodos.

Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Acerca de esta tarea

Puede realizar una copia de seguridad de los datos de un entorno en clúster de NetApp en los siguientes soportes de almacenamiento:

Un dispositivo de cintas conectado directamente a un servidor de archivos NAS

Puede realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente a un servidor de archivos NAS. Este es el método preferido. Por lo general, es más rápido realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente que en una agrupación de almacenamiento de IBM Spectrum Protect utilizando una conexión de red.

Agrupación de almacenamiento en la jerarquía de IBM Spectrum Protect local

Puede realizar una copia de seguridad de los datos en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento de tipo DISK, FILE o de cinta. El ventaja de almacenar los datos en una agrupación de almacenamiento es que puede replicar los datos para lograr una protección de datos adicional. Puede utilizar las agrupaciones de almacenamiento existentes o crear agrupaciones de almacenamiento. Debe tener una conexión de red entre el servidor de archivos NAS y el servidor de IBM Spectrum Protect. La conexión de red debe tener suficiente ancho de banda para transferir los datos de copia de seguridad de NAS.

Consejo: Este tipo de copia de seguridad se denomina a veces una copia de seguridad de archivador a servidor.

Puede utilizar uno de los siguientes métodos de copia de seguridad:

Copia de seguridad de clúster completo

Cuando aplica este método, los datos de copia de seguridad de todo el clúster son propiedad de un único nodo de IBM Spectrum Protect. Aunque mueva los volúmenes dentro del clúster, las operaciones de copia de seguridad del clúster completo continúan y no es necesario reconfigurar las operaciones de copia de seguridad. Este es el método preferido.

Copia de seguridad de clúster parcial

Cuando aplica este método, especifica una máquina virtual de almacenamiento (SVM) de NetApp, que determina el ámbito de la operación de copia de seguridad. La SVM es un servidor virtual que proporciona acceso a parte de un clúster. Puede especificar que cada SVM en el clúster realice una copia de seguridad de los datos en un nodo de IBM Spectrum Protect diferente. Este método requiere una mayor configuración que el método de copia de seguridad de clúster completo, así como una conexión de red para transferir los datos desde la SVM al nodo de IBM Spectrum Protect.

Restricción: No puede utilizar este método para copiar datos en un dispositivo de cintas, porque las SVM no tienen acceso directo a los dispositivos de cintas.

Procedimiento

1. Seleccione el soporte de almacenamiento utilizando las siguientes preguntas:

Pregunta	Soporte de almacenamiento
Según sus requisitos de negocio, ¿es necesario realizar una copia de seguridad de los datos en un dispositivo de cintas local?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Su organización requiere operaciones de copia de seguridad de alta velocidad?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Su organización dispone de suficiente ancho de banda de red para los datos de copia de seguridad de NAS?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente.
¿Su organización desea aumentar la protección de datos mediante la réplica?	Si la respuesta es sí, utilice una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Están los servidores de archivos NAS en ubicaciones remotas sin acceso a las bibliotecas de cintas conectadas directamente?	Si la respuesta es sí, utilice una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.

2. Seleccione un método de copia de seguridad utilizando las siguientes preguntas:

Pregunta	Método de copia de seguridad
Según sus requisitos de negocio, ¿es necesario realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente?	Si la respuesta es sí, utilice el método de copia de seguridad completa. Si la respuesta es no, utilice el método de copia de seguridad completa o parcial.
¿Tiene el sistema suficiente ancho de banda de red para realizar una copia de seguridad de varias SVM sin afectar al rendimiento de red?	Si la respuesta es sí, utilice el método de copia de seguridad completa o parcial. Si la respuesta es no, utilice el método de copia de seguridad completa. El método de copia de seguridad parcial puede afectar negativamente al rendimiento del sistema.
¿Están las SVM distribuidas en varias organizaciones? Por ejemplo, ¿están las SVM controladas por terceros, por ejemplo, por proveedores de plataformas de nube?	Si la respuesta es sí, utilice el método de copia de seguridad parcial, ya que los propietarios de SVM pueden controlar operaciones de copia de seguridad para SVM individuales. Si un propietario de SVM también es propietario de un servidor de IBM Spectrum Protect, el propietario puede configurar operaciones de copia de seguridad desde la SVM en un nodo de servidor. De este modo, el propietario puede controlar el proceso de extremo a extremo. Si la respuesta es no, utilice el método de copia de seguridad completa o parcial.

3. Configure el entorno del sistema en función del soporte de almacenamiento y el método de copia de seguridad que elija. Siga las instrucciones para el método seleccionado:

- Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente
- Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect
- Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect

Consejo: Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, se recomienda reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp. Siga las instrucciones de la sección Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster.

- Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cinta conectado directamente.
- Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.
- Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad parcial de un clúster de NetApp. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos.
- Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster
Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, puede reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp.

Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cinta conectado directamente.

Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetApp, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de todos los volúmenes.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

Acerca de esta tarea

El método recomendado es realizar una copia de seguridad del clúster completo utilizando un nodo y un transportador de datos que estén asociados a la red en todo el clúster. De este modo, se asegura de que los datos de la copia de seguridad pertenezcan a un único nodo de IBM Spectrum Protect. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.

Procedimiento

Para configurar operaciones de copias de seguridad de clúster completo en un dispositivo de cinta conectado directamente, siga estos pasos:

1. Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

2. Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
3. En el servidor de archivos de NetApp, habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
 - a. Habilite las operaciones de copia de seguridad de NDMP con ámbito de SVM en el nivel de clúster. De este modo, inhabilita las operaciones de copia de seguridad de NDMP con ámbito de nodo en el servidor de archivos NAS. Asegúrese de que la opción `node-scoped-ndmp` en el servidor de archivos NAS esté establecida en OFF.
 - b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
 - c. Configure una interfaz de red para las conexiones de control NDMP en el nivel de clúster.
4. Registre el nodo de IBM Spectrum Protect que será propietario de todos los datos de la copia de seguridad del clúster. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio_nas* especifica el dominio del nodo. Asigne el nodo a un dominio que tenga una política para hacer copia de seguridad de datos en una agrupación de almacenamiento apropiada.

5. Determine la dirección IP de la interfaz de gestión de clústeres de NetApp en el servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida del mandato es necesaria si especifica el parámetro HLADDRESS en el paso 6.

6. Defina un transportador de datos para el nodo de IBM Spectrum Protect que será el propietario de los datos de la copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER en una línea:

```
define datamover nombre_transportador_datos type=nascluster  
hladdress=interfaz_gestión_clúster lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz_gestión_clúster* es el valor que ha obtenido en el paso 5 y *nombre_transportador_datos* es el nombre de nodo que ha registrado en el paso 4. Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

Consejo: Después de definir el transportador de datos, los transportadores de datos adicionales se definen automáticamente para cada nodo en el clúster. El nombre de cada transportador de datos coincide con el nombre del nodo físico en el clúster. Utilizará estos transportadores de datos cuando defina vías de acceso a unidades de cintas en el paso 3 de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.

Qué hacer a continuación

Para configurar el dispositivo de cinta para la copia de seguridad del clúster completo, siga las instrucciones de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.

- Configuración de dispositivos de cinta para copias de seguridad de clúster completas
Si tiene previsto realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cintas

conectado directamente, debe configurar el dispositivo de cintas.

Referencia relacionada:

REGISTER NODE (Inscribir un nodo)

Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.

Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de todos los volúmenes del clúster. Todos los datos de la copia de seguridad serán propiedad de un único nodo de IBM Spectrum Protect.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

Procedimiento

1. Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

2. Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
3. Habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
 - a. Habilite NetApp SVM para controlar las operaciones de copia de seguridad de NDMP en el nivel de clúster.
 - b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
 - c. Configure una interfaz de red para las conexiones de control NDMP a nivel de clúster.
4. Registre el nodo de IBM Spectrum Protect que será propietario de todos los datos de la copia de seguridad del clúster. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio_nas* especifica el dominio del nodo.

5. Determine la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida es necesaria si especifica un valor para el parámetro HLADDRESS en el paso 6.

6. Para definir un transportador de datos para el nodo, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASCLUSTER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nascluster  
hladdress=interfaz_gestión_clúster lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz_gestión_clúster* es el valor que ha obtenido en el paso 5 y *nombre_transportador_datos* es el nombre de nodo que ha registrado en el paso 4. Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

7. Configure una política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.

- Actualice el nodo de clúster que ha registrado en el paso 4 en el dominio que se ha configurado en el paso 7. En el servidor de IBM Spectrum Protect, emita el mandato UPDATE NODE:

```
update node nombre_nodo domain=nombre_dominio
```

- Opcional: Identifique los volúmenes en el clúster y planifique las copias de seguridad de los volúmenes:
 - En el servidor de archivos de NAS, identifique los volúmenes del clúster emitiendo el siguiente mandato de Data ONTAP:

```
volume show
```

- Planifique las operaciones de copia de seguridad siguiendo las instrucciones de Planificación de operaciones NDMP.

Qué hacer a continuación

Las tareas siguientes son opcionales:

- Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:
 - En la barra de menús de Centro de operaciones, pulse Clientes.
 - Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
 - Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.
- Para configurar agrupaciones de almacenamiento de copias para la protección de datos añadida, configure la función de cinta a cinta para hacer copias de seguridad de datos. Para ver instrucciones, consulte Copia de seguridad de datos mediante la función de cinta a cinta.

Referencia relacionada:

REGISTER NODE (Inscribir un nodo)

Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad parcial de un clúster de NetApp. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos.

Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de una parte del clúster. Cuando configura una copia de seguridad de clúster parcial, puede determinar el ámbito de la copia de seguridad especificando un servidor virtual, la máquina virtual de almacenamiento (SVM) de NetApp. La SVM proporciona acceso a parte de un clúster.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

Procedimiento

- Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

- Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
- En el servidor de archivos de NetApp, habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
 - Habilite NetApp SVM para controlar las operaciones de copia de seguridad de NDMP.
 - Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
 - Configure una interfaz de red para las conexiones de control NDMP en el nivel de SVM.

4. Registre el nodo de IBM Spectrum Protect que será el propietario de los datos de copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio_nas* especifica el dominio del nodo.

5. Determine la dirección IP numérica o el nombre de dominio de la interfaz de clúster que utiliza SVM. Para determinar el valor, en el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo ONTAP:

```
network interface show -vserver nombre_vserver -role data
```

donde *nombre_vserver* especifica el nombre de la SVM. El valor obtenido es necesario en el paso 6.

6. Para definir un transportador de datos asociado para el nodo de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASVSERVER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nasvserver  
hladdress=interfaz_datos_svm lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz_datos_svm* es el valor que ha obtenido en el paso 5 y *nombre_transportador_datos* es el nombre del nodo que ha registrado en el paso 4.

Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

7. Configure una política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
8. Actualice el nodo que ha registrado en el paso 4 en el dominio que ha configurado en el paso 7. En el servidor de IBM Spectrum Protect, emita el mandato UPDATE NODE:

```
update node nombre_nodo domain=nombre_dominio
```

9. Opcional: identifique los volúmenes en el clúster y planifique las operaciones de copia de seguridad. Realice los pasos siguientes:

- a. En el servidor de archivos de NAS, identifique los volúmenes del clúster emitiendo el siguiente mandato de Data ONTAP:

```
volume show -vserver nombre_vserver
```

donde *nombre_vserver* especifica el nombre de la SVM.

- b. Planifique las operaciones de copia de seguridad siguiendo las instrucciones de Planificación de operaciones NDMP.

Qué hacer a continuación

Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:

1. En la barra de menús de Centro de operaciones, pulse Clientes.
2. Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
3. Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.

Referencia relacionada:

REGISTER NODE (Inscribir un nodo)

Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster

Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, puede reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp.

Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Acerca de esta tarea

Cuando reconfigura IBM Spectrum Protect para utilizar CAB, puede optimizar las operaciones de copia de seguridad de la siguiente manera:

- Puede configurar IBM Spectrum Protect para que realice copias de seguridad de todos los volúmenes de un clúster de NetApp en un dispositivo de cintas conectado directamente o en un servidor de IBM Spectrum Protect. En ambos casos, los datos serán propiedad de un único nodo de IBM Spectrum Protect. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.
- Puede realizar una copia de seguridad parcial de un clúster de NetApp en un servidor de IBM Spectrum Protect. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos. Para establecer el ámbito de una copia de seguridad parcial, especifique una máquina virtual de almacenamiento (SVM) de NetApp, que proporciona acceso a parte de un clúster.

Para reconfigurar IBM Spectrum Protect para utilizar CAB, debe definir un nuevo nodo de IBM Spectrum Protect y un nuevo transportador de datos.

Procedimiento

1. Verifique que se haya instalado NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetApp.
2. Habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

Realice los pasos siguientes:

- a. Habilite las operaciones de copia de seguridad de NDMP con ámbito de SVM en el nivel de clúster. De este modo, inhabilita las operaciones de copia de seguridad de NDMP con ámbito de nodo en el servidor de archivos NAS. Asegúrese de que la opción `node-scoped-ndmp` en el servidor de archivos NAS esté establecida en OFF.
- b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
- c. Configure una interfaz de red para las conexiones de control NDMP a nivel de clúster.

Para una copia de seguridad de clúster parcial

Realice los pasos siguientes:

- a. Habilite NDMP con ámbito de SVM para controlar las operaciones de copia de seguridad de NDMP.
- b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
- c. Configure una interfaz de red para las conexiones de control NDMP en el nivel de SVM.

3. Registre el nodo de IBM Spectrum Protect que será el propietario de los datos de copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio_nas* especifica el dominio del nodo.

4. Si tiene previsto realizar una copia de seguridad de un clúster completo, determine la dirección IP de la interfaz de gestión de clústeres de NetApp en el servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida es necesaria si especifica el parámetro HLADDRESS en el paso 6.

5. Si va a realizar una copia de seguridad de un clúster parcial, determine la dirección IP numérica o el nombre de dominio de la interfaz de clúster que utiliza SVM. Para determinar el valor, emita el siguiente mandato de sistema operativo Data ONTAP en el servidor de archivos de NAS:

```
network interface show -vserver nombre_vserver -role data
```

donde *nombre_vserver* especifica el nombre de la SVM. El valor que obtiene es necesario en el paso 6.

6. Defina un transportador de datos para el nodo de IBM Spectrum Protect. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

Defina un transportador de datos para el nodo de IBM Spectrum Protect que será el propietario de los datos de la copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER en una línea:

```
define datamover nombre_transportador_datos type=nascluster  
hladdress=interfaz_gestión_clúster lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```


donde *interfaz_gestión_clúster* es el valor que ha obtenido en el paso 4 y *nombre_transportador_datos* es el nombre de nodo que ha registrado en el paso 3.

Consejo: Después de definir el transportador de datos, los transportadores de datos adicionales se definen automáticamente para cada nodo en el clúster. El nombre de cada transportador de datos coincide con el nombre del nodo físico en el clúster. Utilizará estos transportadores de datos cuando defina vías de acceso a unidades de cintas que están conectadas al clúster.

Para una copia de seguridad de clúster parcial

Para definir un transportador de datos para el nodo, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASVSERVER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nasvserver
hladdress=interfaz_datos_svm lladdress=puerto
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz_datos_svm* es el valor que ha obtenido en el paso 5 y *nombre_transportador_datos* es el nombre de nodo que ha registrado en el paso 3.

Para obtener información sobre cómo especificar otros parámetros en el mandato DEFINE DATAMOVER, consulte DEFINE DATAMOVER (Definir un transportador de datos).

7. Para realizar una copia de seguridad de los datos en un dispositivo de cinta conectado directamente, para cada unidad de cintas que está conectada al clúster, identifique el nombre de dispositivo y el nodo físico al que está conectada la unidad:
 - a. En el servidor de archivos de NAS, emita el siguiente mandato de Data ONTAP:

```
storage tape show-tape-drive
```

- b. Revise la salida para encontrar el número de serie de la unidad de cintas y el nodo del clúster al que se conecta la unidad. La misma stanza incluye el nombre de dispositivo, por ejemplo, *st1*, *st2* o *st3*.

8. Para configurar una copia de seguridad de clúster completa en un dispositivo de cinta conectado directamente, siga las instrucciones de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.
9. Para configurar una copia de seguridad de clúster completa o parcial en un servidor de IBM Spectrum Protect, configure una política para gestionar las copias de seguridad de imagen de NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
10. Inhabilite las operaciones de copia de seguridad planificadas para todos los nodos que se han utilizado previamente para realizar una copia de seguridad del clúster de NetApp.
11. Identifique los volúmenes en el clúster y, opcionalmente, planifique las operaciones de copia de seguridad de los volúmenes. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

- a. En el servidor de archivos de NAS, identifique los volúmenes del clúster utilizando el siguiente mandato de Data ONTAP:

```
volume show
```

- b. Ejecutar una copia de seguridad completa de todo el clúster.
 - c. Opcional: para planificar operaciones de copia de seguridad, siga las instrucciones de Planificación de operaciones NDMP.

Para una copia de seguridad de clúster parcial

- a. En el servidor de archivos de NAS, identifique los volúmenes del clúster utilizando el siguiente mandato de Data ONTAP:

```
volume show -vserver nombre_vserver
```

donde *nombre_vserver* especifica el nombre de la SVM.

- b. Ejecutar una copia de seguridad completa del clúster parcial.
 - c. Opcional: para planificar operaciones de copia de seguridad, siga las instrucciones de Planificación de operaciones NDMP.

Qué hacer a continuación

Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:

1. En la barra de menús de Centro de operaciones, pulse Clientes.
2. Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
3. Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.

Referencia relacionada:

DEFINE DATAMOVER (Definir un transportador de datos)
DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)
REGISTER NODE (Inscribir un nodo)

Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP

Después de configurar IBM Spectrum Protect para operaciones NDMP, está listo para empezar a utilizar NDMP.

Procedimiento

Utilice una interfaz de cliente o una interfaz de administración para realizar una copia de seguridad de imagen del sistema de archivos. Por ejemplo, para utilizar la interfaz de cliente de copia de seguridad/archivado de Windows con el fin de realizar una copia de seguridad de un sistema de archivos denominado /vol/vol1 en un servidor de archivos NAS denominado NAS1, emita el siguiente mandato:

```
dsmc backup nas -nasnodename=nas1 {/vol/vol1}
```

Para obtener más información acerca del mandato, consulte Imagen de copia de seguridad.

Consejo: Cuando utilice la interfaz de cliente, se le solicitará que se autentique como administrador de IBM Spectrum Protect antes de que pueda empezar la operación. El ID de administrador debe tener como mínimo autorización de propietario de cliente para el nodo NAS.

Puede realizar la misma operación de copia de seguridad con una interfaz de servidor. Por ejemplo, desde el cliente de línea de mandatos de administración, haga una copia de seguridad del sistema de archivos denominado /vol/vol1 en un servidor de archivos NAS denominado NAS1, emitiendo el siguiente mandato:

```
backup node nas1 /vol/vol1
```

Restricción: Los mandatos BACKUP NAS y BACKUP NODE no incluyen instantáneas. Para hacer copias de seguridad de instantáneas, consulte el apartado Copia de seguridad y restauración con instantáneas.

Puede restaurar la imagen utilizando cualquiera de las dos interfaces. Las copias de seguridad son idénticas tanto si la copia de seguridad se efectúa con una interfaz de cliente como con una interfaz de servidor. Por ejemplo, supongamos que desea restaurar la imagen de la que ha hecho copia de seguridad en los ejemplos anteriores. En este ejemplo, el sistema de archivos denominado /vol/vol1 se va a restaurar en /vol/vol2. Restaure el sistema de archivos con el mandato siguiente, que emitirá desde una interfaz de cliente de copia de seguridad/archivado Windows:

```
dsmc restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}
```

Puede elegir restaurar el sistema de archivos mediante una interfaz de servidor. Por ejemplo, para restaurar el nombre de sistema de archivos /vol/vol1 en el sistema de archivos /vol/vol2, para un servidor de archivos NAS denominado NAS1, especifique el mandato siguiente:

```
restore node nas1 /vol/vol1 /vol/vol2
```

Puede restaurar datos de un sistema NAS de un proveedor a un sistema NAS de otros proveedores al utilizar el formato de datos NDMPDUMP. Sin embargo, debe verificar la compatibilidad entre sistemas o mantener una agrupación de almacenamiento diferente para cada proveedor de NAS.

- Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único
Si tiene varios servidores NAS en diversas ubicaciones, es posible que prefiera enviar los datos de la copia de seguridad a un único servidor de IBM Spectrum Protect que conectar una biblioteca de cintas a cada dispositivo NAS.
- Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect
Puede hacer copias de seguridad de los datos en un único servidor de IBM Spectrum Protect en lugar de conectar una biblioteca de cintas con cada dispositivo NAS.

Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único

Si tiene varios servidores NAS en diversas ubicaciones, es posible que prefiera enviar los datos de la copia de seguridad a un único servidor de IBM Spectrum Protect que conectar una biblioteca de cintas a cada dispositivo NAS.

Cuando se almacenan datos de copia de seguridad de NAS en la jerarquía de almacenamiento del servidor de IBM Spectrum Protect, puede aplicar funciones de gestión de datos de programa de fondo de IBM Spectrum Protect. De este modo, puede aprovechar las características de migración, reclamación, recuperación tras desastre y otras.

Para realizar la copia de seguridad de un dispositivo de NAS en una agrupación de almacenamiento nativa de IBM Spectrum Protect, establezca la agrupación de almacenamiento de destino del grupo de copias para que apunte a la agrupación de almacenamiento nativa deseada. Dicha agrupación proporciona información acerca de la biblioteca y las unidades que se utilizan para realizar las operaciones de copia de seguridad y restauración. Asegúrese de que la agrupación de almacenamiento de destino disponga de espacio suficiente para los datos de NAS, de los que se puede hacer una copia de seguridad en dispositivos de tipo secuencial, de disco o de archivo. No es preciso definir otra clase de dispositivo.

Si va a crear una tabla de contenido, deberá especificar una clase de gestión en el con el parámetro TOCDESTINATION de los mandatos DEFINE y UPDATE COPYGROUP. Al realizar una copia de seguridad del servidor de archivos de NAS en agrupaciones nativas de IBM Spectrum Protect, el TOCDESTINATION puede ser el mismo que el del destino de los datos de los que se hace copia de seguridad utilizando NDMP.

Las consideraciones de cortafuegos son más estrictas que en el caso del método de archivador a biblioteca conectada, ya que tanto el servidor de IBM Spectrum Protect como el servidor de archivos NAS pueden iniciar las comunicaciones. Los servidores de cintas NDMP se ejecutan como hebras dentro del servidor de IBM Spectrum Protect y el servidor de cintas acepta conexiones en el puerto 10001. Este número de puerto se puede cambiar mediante la opción siguiente del archivo de opciones del servidor de IBM Spectrum Protect: NDMPPORTRANGE número_puerto_bajo, número_puerto_alto.

Durante las operaciones de copia de seguridad de archivador a servidor de NDMP, puede utilizar la opción NDMPREFDATAINTERFACE para especificar qué interfaz de red utiliza el servidor de IBM Spectrum Protect para recibir datos de copia de seguridad. El valor de esta opción es un nombre de host o una dirección IPV4 que se asocia a una de las interfaces de red activas del sistema en el que se ejecuta el servidor de IBM Spectrum Protect. Esta interfaz debe haberse activado para IPV4.

Antes de usar esta opción, verifique que el dispositivo NAS dé soporte a las operaciones NDMP que usan una interfaz de red distinta para las conexiones de control NDMP y de datos NDMP. IBM Spectrum Protect usa conexiones de control NDMP para autenticar un servidor NDMP y supervisar una operación NDMP, mientras que se usan conexiones de datos NDMP para transmitir y recibir datos de copia de seguridad durante las operaciones NDMP. Aún debe configurar el dispositivo NAS para direccionar los datos de copia de seguridad y restauración a la interfaz de red apropiada.

Cuando se habilita, la opción NDMPREFDATAINTERFACE afecta a todas las operaciones de gestor de archivos a servidor NDMP posteriores. No afecta a las conexiones de control NDMP, ya que estas usan la interfaz de red predeterminada del sistema. Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Los servidores de archivos NetApp proporcionan una opción NDMP (ndmpd.preferred_interface) para cambiar la interfaz usada para las conexiones de datos NDMP. Para obtener más información, consulte la documentación del dispositivo NAS.

Para obtener instrucciones sobre cómo realizar operaciones de copia de seguridad de archivador a servidor NDMP, consulte Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect.

Para obtener información sobre las opciones de servidor, consulte Opciones de servidor.

Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect

Puede hacer copias de seguridad de los datos en un único servidor de IBM Spectrum Protect en lugar de conectar una biblioteca de cintas con cada dispositivo NAS.

Procedimiento

Para realizar copias de seguridad de un servidor en un sistema de archivos NAS, complete los pasos siguientes:

1. Seleccione una agrupación de almacenamiento existente o configure una agrupación de almacenamiento para los datos NAS emitiendo el siguiente mandato:

```
define stgpool naspool disk
```

2. Defina volúmenes para agregarlos a la agrupación de almacenamiento. Por ejemplo, defina un volumen denominado naspool_volAB:

```
define volume naspool /usr/storage/naspool_volAB formatsize=100
```

3. Establezca el destino de la copia en la agrupación de almacenamiento definida previamente y active el conjunto de políticas asociadas.

```
update copygroup standard standard standard destination=naspool  
tocdestination=naspool  
activate policysset standard standard
```

El destino de los datos NAS está determinado por el destino del grupo de copia. El cálculo del tamaño del almacenamiento en el caso de las copias de seguridad diferenciales NAS emplea la ocupación del espacio de archivos, el mismo valor que se utiliza para realizar una copia de seguridad completa. Puede utilizar este cálculo del tamaño como una de las consideraciones que deben tenerse en cuenta al elegir una agrupación de almacenamiento. Uno de los atributos de una agrupación de almacenamiento es el valor MAXSIZE, que indica que los datos se envíen a la agrupación de almacenamiento NEXT si el tamaño calculado es superior al valor MAXSIZE. Dado que las copias de seguridad diferenciales NAS a las agrupaciones de almacenamiento nativas de IBM Spectrum Protect utilizan el tamaño de ocupación del espacio del archivo base como cálculo del tamaño del almacenamiento, las copias de seguridad diferenciales acaban en la misma agrupación de almacenamiento que la copia de seguridad completa. Según los valores de proximidad, las copias de seguridad diferenciales pueden acabar en los mismos medios que la copia de seguridad completa.

4. Configure un nodo y un transportador de datos para el dispositivo NAS. El formato de datos significa que las imágenes de copia de seguridad creadas por este dispositivo NAS son un tipo de volcado de la imagen de copia de seguridad en un formato específico de NetApp.

```
register node nas1 nas1 type=nas domain=standard
define datamover nas1 type=nas hla=nas1 user=root
password=***** dataformat=netappdump
```

Ahora ya se puede realizar la copia de seguridad del dispositivo NAS en una agrupación de almacenamiento del servidor de IBM Spectrum Protect. Las vías de acceso se pueden definir en unidades locales, pero el destino especificado mediante la clase de gestión determina la ubicación de destino de esta operación de copia de seguridad.

5. Realice la copia de seguridad del dispositivo NAS en la agrupación de almacenamiento de IBM Spectrum Protect ejecutando el mandato siguiente:

```
backup node nas1 /vol/vol0
```

6. Restaure un dispositivo NAS de la agrupación de almacenamiento de IBM Spectrum Protect ejecutando el mandato siguiente:

```
restore node nas1 /vol/vol0
```

Copia de seguridad y restauración en nivel de archivo para operaciones NDMP

Al realizar una copia de seguridad de los datos utilizando NDMP, puede especificar que el servidor de IBM Spectrum Protect recopile y almacene información de nivel de archivo en una tabla de contenido (TOC).

Si especifica esta opción al realizar la copia de seguridad, posteriormente puede visualizar la TOC de la imagen de copia de seguridad. Mediante el cliente web de archivado y copia de seguridad, puede seleccionar archivos o directorios individuales para restaurarlos directamente de las imágenes de copia de seguridad generadas.

Para recopilar información de nivel de archivo, se necesita tiempo de proceso, recursos de red, espacio de agrupación de almacenamiento y espacio de base de datos temporal extras, así como posiblemente interacción adicional entre dispositivos de almacenamiento. Para obtener instrucciones sobre la configuración de dispositivos de almacenamiento, consulte Configuración de dispositivos de almacenamiento. Considere la posibilidad de destinar más espacio a la base de datos del servidor de IBM Spectrum Protect. Debe configurar la política de modo que el servidor de IBM Spectrum Protect almacene la TOC en una agrupación de almacenamiento distinta de la empleada para almacenar la imagen de copia de seguridad. La TOC se maneja del mismo modo que cualquier otro objeto de esa agrupación de almacenamiento.

También tiene la posibilidad de efectuar una copia de seguridad mediante NDMP sin recopilar información de restauración de nivel de archivo.

Para permitir que se cree una TOC para una copia de seguridad mediante NDMP, debe definir el atributo TOCDESTINATION en el grupo de copias de seguridad para la clase de gestión a la que está vinculada esta imagen de copia de seguridad. No puede especificar una agrupación de almacenamiento de copia ni una agrupación de datos activos como destino. La agrupación de almacenamiento que especifique para el destino de la tabla de contenido debe tener un formato de datos NATIVE o NONBLOCK, por lo tanto no puede ser la agrupación de almacenamiento en cinta empleada para la imagen de copia de seguridad.

Si elige recopilar la información de nivel de archivo, especifique el parámetro TOC en el mandato de servidor BACKUP NODE. O bien, si inicia la copia de seguridad utilizando el cliente, puede especificar la opción TOC en el archivo de opciones de cliente, en el conjunto de opciones de cliente o en la línea de mandatos del cliente. Puede especificar NO, PREFERRED o YES. Si especifica PREFERRED o YES, el servidor de IBM Spectrum Protect almacena la información de archivo de una única copia de seguridad controlada por NDMP en una TOC. La TOC se coloca en una agrupación de almacenamiento. A continuación, el servidor de IBM Spectrum Protect puede acceder a la TOC de modo que el servidor o cliente pueda consultar la información de archivo y directorio. El uso del parámetro TOC permite generar una TOC para unas imágenes y no otras, sin que se necesiten clases de gestión distintas para las imágenes.

Para obtener más información sobre el mandato BACKUP NODE, consulte BACKUP NODE (Copia de seguridad de un nodo NAS).

Para evitar retardos de montaje y asegurarse de que tiene suficiente espacio disponible, utilice agrupaciones de almacenamiento de acceso aleatorio (clase de dispositivo DISK) como destino para la TOC. Para las agrupaciones de almacenamiento de acceso secuencial, no es necesario etiquetar los volúmenes ni realizar ninguna otra tarea de preparación si los volúmenes reutilizables están permitidos.

Para obtener más información, consulte Gestión de tablas de contenido.

- Interfaces para las operaciones de restauración a nivel de archivos
Al restaurar directorios y archivos individuales, tiene la opción de utilizar una de dos interfaces para iniciar la restauración: el cliente web de archivado y copia de seguridad o la interfaz de servidor.
- Caracteres internacionales para servidores de archivos NetApp
Todos los sistemas que crean datos en un volumen de servidor de archivos NAS específico, o que acceden a sus datos, deben hacerlo de modo compatible con el valor de idioma del volumen.
- Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio
Las operaciones de restauración a nivel de archivos se admiten para imágenes de copia de seguridad a nivel de directorio.

Interfaces para las operaciones de restauración a nivel de archivos

Al restaurar directorios y archivos individuales, tiene la opción de utilizar una de dos interfaces para iniciar la restauración: el cliente web de archivado y copia de seguridad o la interfaz de servidor.

Operaciones de restauración mediante el cliente web de copia de seguridad-archivado.

El cliente web del archivado y copia de seguridad requiere que existe una TOC para restaurar archivos y directorios. El cliente web debe estar en un sistema Windows. El servidor de IBM Spectrum Protect accede a la TOC desde la agrupación de almacenamiento y carga la información de la tabla de contenido en una tabla de base de datos temporal. A continuación, puede utilizar el cliente web de archivado y copia de seguridad para examinar los directorios y archivos incluidos en una o varias imágenes de sistemas de archivos, y seleccionar directorios o archivos individuales para restaurarlos directamente a partir de las imágenes de copia de seguridad generadas.

Operaciones de restauración mediante la interfaz de servidor

- Si dispone de una TOC, utilice el mandato QUERY NASBACKUP para visualizar información sobre las imágenes de copia de seguridad generadas por NDMP y para ver qué imágenes tienen su correspondiente TOC. Después, utilice el mandato RESTORE NODE con el parámetro FILELIST.
- Si no ha creado una TOC, el contenido de la imagen de copia de seguridad no podrá visualizarse. Puede restaurar archivos y directorios individuales si sabe el nombre del archivo o directorio y en qué imagen se encuentra la copia de seguridad. Utilice el mandato RESTORE NODE con el parámetro FILELIST.

Caracteres internacionales para servidores de archivos NetApp

Todos los sistemas que crean datos en un volumen de servidor de archivos NAS específico, o que acceden a sus datos, deben hacerlo de modo compatible con el valor de idioma del volumen.

Para obtener plena compatibilidad para los caracteres internacionales en los nombres de archivos y directorios, debe instalar Data ONTAP 6.4.1 o posterior, si está disponible, en el servidor de archivos de NetApp NAS.

Si el nivel de Data ONTAP de que dispone es anterior a 6.4.1, debe tener una de las dos configuraciones siguientes para recopilar y restaurar información de nivel de archivo. El uso de configuraciones distintas a estas dos puede ocasionar resultados imprevisibles. El servidor de IBM Spectrum Protect emitirá un mensaje de aviso (ANR4946W) durante las operaciones de copia de seguridad. El mensaje indica que la codificación de caracteres de los mensajes históricos de archivo NDMP es desconocida y se dará por supuesta la codificación UTF-8 para construir una tabla de contenido. El omitir este mensaje no supone ningún riesgo únicamente en las dos configuraciones siguientes.

- Los datos tienen nombres de archivo y de directorio que contienen caracteres en inglés únicamente (ASCII de 7 bits).
- Los datos tienen nombres de directorio y archivo que contienen caracteres que no están en inglés y el idioma del volumen se ha establecido en la versión de UTF-8 del entorno nacional adecuado (por ejemplo, de UTF-8 para el alemán).

Si el nivel de Data ONTAP de que dispone es 6.4.1 o posterior, debe tener una de las tres configuraciones siguientes para recopilar y restaurar información de nivel de archivo. El uso de configuraciones distintas a estas tres puede ocasionar resultados imprevisibles.

- Los datos tienen nombres de directorio y archivo que contienen caracteres en inglés únicamente (ASCII de 7 bits) y el idioma del volumen no se ha establecido o se ha establecido en uno de estos valores:
 - C (POSIX)
 - en
 - en_US
 - en.UTF-8

- `en_US.UTF-8`
- Los datos tienen nombres de directorio y archivo que contienen caracteres que no están en inglés y el idioma del volumen se ha establecido en el entorno nacional adecuado (por ejemplo, `de.UTF-8` o `de` para el alemán).
Consejo: El uso de la versión de UTF-8 del valor de idioma del volumen es más eficaz en términos de proceso del servidor de IBM Spectrum Protect y espacio de almacenamiento de la tabla de contenido.
- Utilice CIFS únicamente para crear los datos y acceder a ellos.

Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio

Las operaciones de restauración a nivel de archivos se admiten para imágenes de copia de seguridad a nivel de directorio.

Al igual que con una copia de seguridad de sistema de archivos NAS, se crea una tabla de contenidos durante una acción de copia de seguridad a nivel de directorio, y puede examinar los archivos de la imagen utilizando el cliente web. La forma predeterminada es que los archivos se restauren a la ubicación original. Sin embargo, durante una restauración a nivel de archivos a partir de la copia de seguridad a nivel de directorios, puede seleccionar un sistema de archivos distinto u otro nombre del espacio de archivos virtual como destino.

Para una tabla de contenidos (TOC) de una imagen de copia de seguridad a nivel de directorio, los nombres de vía de acceso para todos los archivos son relativos al directorio especificado en la definición de espacio de archivos virtual, no la raíz del sistema de archivos.

Operaciones de copia de seguridad y restauración a nivel de directorio

Si tiene un sistema de archivos NAS grande, al iniciar una copia de seguridad a nivel de directorios se reducen los tiempos de copia de seguridad y restauración y se proporciona más flexibilidad en la configuración de copias de seguridad NAS. Al definir los espacios de archivos virtuales, la copia de seguridad del sistema de archivos se debe partir en varias operaciones de copia de seguridad NDMP y varias unidades de cintas. También puede utilizar distintas planificaciones de copia de seguridad con el fin de realizar una copia de seguridad de subárboles de un sistema de archivos.

El nombre del espacio de archivos virtual no puede ser idéntico a ningún sistema de archivos en el nodo NAS. Si se crea un sistema de archivos en el dispositivo NAS con el mismo nombre que un sistema de archivos virtual, se producirá un conflicto de nombres en el servidor de IBM Spectrum Protect al realizarse la copia de seguridad del nuevo espacio de archivos. Para obtener instrucciones sobre cómo emitir mandatos de correlación de espacios de archivos virtuales, consulte `DEFINE VIRTUALFSMAPPING` (Definir una correlación de espacios de archivos virtuales).

Restricción: Las correlaciones de espacios de archivos virtuales sólo se admiten para nodos NAS.

- Copia de seguridad y restauración a nivel de directorio para operaciones NDMP
El mandato `DEFINE VIRTUALFSMAPPING` correlaciona una vía de acceso de directorios de un servidor de archivos NAS con un nombre de espacio de archivos virtual en el servidor de IBM Spectrum Protect. Tras definir la correlación, puede llevar a cabo operaciones NAS como `BACKUP NODE` y `RESTORE NODE` utilizando los nombres de espacios de archivos virtuales como si se tratase de espacios de archivos NAS reales.
- Copia de seguridad y restauración con instantáneas
Las operaciones de copia de seguridad a nivel de directorio NDMP le ofrecen la posibilidad de realizar una copia de seguridad de las instantáneas creadas por el usuario de un sistema de archivos NAS. Estas instantáneas se almacenan como subdirectorios. Las instantáneas se pueden tomar en cualquier momento, y la copia de seguridad se puede aplazar hasta un momento más adecuado.

Copia de seguridad y restauración a nivel de directorio para operaciones NDMP

El mandato `DEFINE VIRTUALFSMAPPING` correlaciona una vía de acceso de directorios de un servidor de archivos NAS con un nombre de espacio de archivos virtual en el servidor de IBM Spectrum Protect. Tras definir la correlación, puede llevar a cabo operaciones NAS como `BACKUP NODE` y `RESTORE NODE` utilizando los nombres de espacios de archivos virtuales como si se tratase de espacios de archivos NAS reales.

Para iniciar una copia de seguridad del directorio, emita el mandato `BACKUP NODE` y especifique el nombre del espacio de archivos virtual en lugar del nombre de un espacio de archivos. Para restaurar el subárbol de directorios a la ubicación original, ejecute el mandato `RESTORE NODE` y especifique el nombre del espacio de archivos virtual.

Las definiciones de espacios de archivos virtuales también pueden especificarse como destino en un mandato `RESTORE NODE`. De esta forma, podrá restaurar imágenes de copia de seguridad (del sistema de archivos o directorio) en un directorio de cualquier sistema de archivos del dispositivo NAS.

Puede utilizar el cliente web para seleccionar archivos con el fin de restaurarlos a partir de una imagen de copia de seguridad de nivel de directorios porque el cliente de IBM Spectrum Protect trata los nombres de espacios de archivos virtuales como espacios de archivos NAS.

Copia de seguridad y restauración con instantáneas

Las operaciones de copia de seguridad a nivel de directorio NDMP le ofrecen la posibilidad de realizar una copia de seguridad de las instantáneas creadas por el usuario de un sistema de archivos NAS. Estas instantáneas se almacenan como subdirectorios. Las instantáneas se pueden tomar en cualquier momento, y la copia de seguridad se puede aplazar hasta un momento más adecuado.

Procedimiento

Por ejemplo, para realizar una copia de seguridad de una instantánea que se ha creado para un sistema de archivos NetApp, complete los pasos siguientes:

1. En la consola del dispositivo NAS, emita el mandato para crear la instantánea. SNAP CREATE es el mandato para un dispositivo NetApp.

```
snap create vol2 february17
```

Este ejemplo creará una instantánea denominada FEBRUARY 17 del sistema de archivos /vol/vol2. La ubicación física para los datos de la instantánea es el directorio /vol/vol2/.snapshot/february17. La ubicación de almacenamiento de los datos de instantánea dependerá de la implementación del proveedor NAS. Para NetApp, se puede utilizar el mandato SNAP LIST para visualizar todas las instantáneas de un determinado sistema de archivos.

2. Defina una definición de correlación de espacios de archivos virtuales en el servidor de IBM Spectrum Protect para los datos de la instantánea creados en el paso anterior.

```
define virtualfsmapping nas1 /feb17snapshot /vol/vol2 /.snapshot/february17
```

Este ejemplo creará una definición de correlación de espacios de archivos virtuales denominada /feb17snapshot.

3. Realice una copia de seguridad de la correlación de espacios de archivos virtuales.

```
backup node nas1 /feb17snapshot mode=full toc=yes
```

4. Tras crear la copia de seguridad, puede restaurar toda la imagen instantánea o un archivo individual. Antes de restaurar los datos, puede crear un nombre de correlación de espacios de archivos virtuales para el directorio de destino. Puede elegir cualquier nombre del sistema de archivos como destino. La ubicación de destino en este ejemplo es el directorio /feb17snaprestore del sistema de archivos /vol/vol1.

```
define virtualfsmapping nas1 /feb17snaprestore /vol/vol1 /feb17snaprestore
```

5. Restaure la imagen de copia de seguridad de instantánea.

```
restore node nas1 /feb17snapshot /feb17snaprestore
```

De esta forma se restaura una copia del sistema de archivos /vol/vol2 en el directorio /vol/vol1/feb17snaprestore en el mismo estado que tenía cuando se creó la instantánea en el primer paso.

Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape

Puede realizar una copia de seguridad de sistemas de archivos NetApp grandes utilizando la característica NetApp SnapMirror to Tape (también denominada SMTape). Si se usa una copia de datos a nivel de bloque para copia de seguridad, el método SnapMirror to Tape es más rápido que una copia de seguridad completa tradicional NDMP y se puede usar si las copias de seguridad completas de NDMP no resultan prácticas.

Utilice la característica NDMP SnapMirror to Tape como una opción de recuperación tras desastre para copiar sistemas de archivos NetApp grandes en almacenamiento auxiliar. En la mayoría de los sistemas de archivos NetApp, utilice el método de copia de seguridad diferencial o completa NDMP estándar.

Mediante la especificación de un parámetro en los mandatos BACKUP NODE y RESTORE NODE, puede hacer una copia de seguridad de los sistemas de archivos y restaurarlos utilizando SnapMirror to Tape. Hay diversas limitaciones y restricciones sobre cómo pueden usarse las imágenes de SnapMirror. Tenga en cuenta las siguientes directrices antes de usarlas como un método de copia de seguridad:

- Si ha instalado NetApp ONTAP 8.2 o posterior, debe definir un transportador de datos de tipo NASCLUSTER o NASVSERVER para operaciones de SnapMirror to Tape.

- No puede iniciar una copia de seguridad de SnapMirror to Tape o una operación de restauración desde IBM Spectrum Protect Centro de operaciones, el cliente web o el cliente de línea de mandatos.
- No se pueden realizar copias de seguridad diferenciales de imágenes de SnapMirror.
- No puede realizar una copia de seguridad de nivel de directorio utilizando SnapMirror to Tape. Por consiguiente, IBM Spectrum Protect no permite operaciones de copia de seguridad de SnapMirror to Tape en un espacio de archivos virtual de servidor.
- No se puede realizar una operación de restauración a nivel de archivo NDMP desde imágenes de SnapMirror to Tape. Por lo tanto, nunca se crea una tabla de contenidos durante las copias de seguridad de imágenes de SnapMirror to Tape.
- Al inicio de la operación de copia de SnapMirror to Tape, el servidor de archivos genera una instantánea del sistema de archivos. NetApp proporciona una variable de entorno de NDMP para controlar si esta instantánea se elimina al final de la operación de SnapMirror to Tape. IBM Spectrum Protect siempre establece esta variable para eliminar la instantánea.
- Tras recuperar una imagen de SnapMirror to Tape y copiarla en un sistema de archivos NetApp, el sistema de archivos de destino sigue configurado como socio de SnapMirror. NetApp proporciona una variable de entorno NDMP para controlar si esta relación de SnapMirror se debe romper. IBM Spectrum Protect siempre "rompe" la relación de SnapMirror durante la recuperación. Tras completarse la operación de restauración, el sistema de archivos de destino está en el mismo estado que el sistema de archivos original en el momento de la copia de seguridad.

Para obtener más información sobre la función SnapMirror to Tape, consulte BACKUP NODE (Copia de seguridad de un nodo NAS) y RESTORE NODE (Restaurar un nodo NAS).

Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra

Cuando el servidor de IBM Spectrum Protect inicia una operación de copia de seguridad NDMP en un transportador de datos Celerra, la copia de seguridad de un sistema de archivos grande puede tardar varias horas en realizarse. Sin los puntos de comprobación integrados de Celerra, los cambios que se producen en el sistema de archivos se graban en la imagen de copia de seguridad.

Como resultado, la imagen de copia de seguridad incluye los cambios realizados en el sistema de archivos durante la operación de copia de seguridad entera. La imagen de copia de seguridad no es una imagen de punto en el tiempo verdadera del sistema de archivos.

Si está realizando operaciones de copia de seguridad de NDMP desde servidores de archivos de Celerra, actualice el sistema operativo del transportador de datos a la versión de servidor de archivos de Celerra T5.5.25.1 o posterior. Esta versión del sistema operativo permite habilitar los puntos de comprobación integrados para todas las operaciones de copia de seguridad NDMP desde Celerra Control Workstation. Al habilitar esta característica se asegura de que los datos de copia de seguridad representen verdaderas imágenes de punto en el tiempo del sistema de archivos del que se hace copia de seguridad.

Para obtener instrucciones sobre cómo habilitar los puntos de comprobación integrados durante todas las operaciones de copia de seguridad de NDMP, consulte la documentación de servidor de archivos de Celerra.

Si la versión del sistema operativo del servidor de archivos Celerra es anterior a la versión T5.5.25.1 y se usa NDMP para la copia de seguridad de los transportadores de datos Celerra, debe generar manualmente una instantánea del sistema de archivos usando la característica de punto de comprobación de la línea de mandatos de Celerra. A continuación, inicie una operación de copia de seguridad de NDMP del sistema de archivos de punto de comprobación en lugar del sistema de archivos original.

Consulte la documentación del servidor de archivos de Celerra para obtener instrucciones sobre la creación y planificación de puntos de control desde la estación de trabajo de control de Celerra.

Réplica de los nodos NAS

Puede replicar un nodo NAS que utiliza NDMP para operaciones de copia de seguridad. Antes de configurar la operación de réplica, revise las restricciones que se aplican.

Acerca de esta tarea

Restricciones:

- Los datos de copia de seguridad deben estar en una agrupación de almacenamiento con el formato de datos NATIVE. No puede replicar datos de copia de seguridad en agrupaciones de almacenamiento que tienen los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
- Una copia de seguridad diferencial sólo puede replicarse si se replica su copia de seguridad completa.

Procedimiento

1. Habilite el nodo NAS para la réplica emitiendo el mandato UPDATE NODE:

```
update node nombre_nodo replstate=enabled
```

donde *nombre_nodo* especifica el nombre del nodo NAS.

2. Replique el nodo emitiendo el mandato REPLICATE NODE:

```
replicate node nombre_nodo
```

donde *nombre_nodo* especifica el nombre del nodo NAS.

3. Para garantizar que los datos replicados puedan restaurarse, defina un transportador de datos en el servidor de destino para el nodo emitiendo el mandato DEFINE DATAMOVER:

```
define datamover nombre_nodo type=nas hladdress=dirección_hl lladdress=dirección_ll  
userid=ID_usuario password=contraseña_usuario dataformat=netappdump
```

donde:

nombre_nodo

Especifica el nombre del nodo NAS.

dirección_hl

Especifica la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS.

dirección_ll

Especifica el número de puerto TCP para acceder al dispositivo NAS para las sesiones NDMP.

ID_usuario

Especifica el ID del usuario autorizado para iniciar una sesión con el servidor de archivos NAS.

contraseña_usuario

Especifica la contraseña del usuario autorizado para iniciar una sesión NDMP con el servidor de archivos NAS.

Resultados

El formato de los datos de copia de seguridad no cambia durante el proceso de réplica. Si los datos de copia de seguridad se replican, la tabla de contenido asociada también se replican.

Protección de datos utilizando la característica con licencia NetApp SnapLock

Puede utilizar la característica con licencia NetApp SnapLock para cumplir los estrictos requisitos normativos. Al habilitar la característica SnapLock, puede utilizar IBM Spectrum Protect para establecer una fecha de retención de los archivos y aplicar un estado WORM (Grabar una vez, leer varias) a un archivo.

Los datos almacenados con una fecha de retención no pueden suprimirse del sistema de archivos antes de que caduque el periodo de retención. La función SnapLock puede utilizarse únicamente con servidores de IBM Spectrum Protect que tengan habilitada la protección de retención de datos.

Los datos archivados por servidores con protección de retención de datos y almacenados en servidores de archivos NetApp NAS se almacenan como volúmenes FILE de IBM Spectrum Protect. Al final de una transacción de grabación, se establece una fecha de retención para el volumen FILE a través de la interfaz SnapLock. Esta fecha se calcula mediante los parámetros RETVER y RETMIN del grupo de copias archivadas utilizado al archivar los datos. Al asociar una fecha de retención con el volumen FILE, este volumen no destruirá ni sobrescribirá los datos hasta que pase la fecha de retención. Este tipo de volúmenes FILE se conocen como volúmenes WORM FILE. Tras establecer una fecha de retención, no se puede suprimir el volumen WORM FILE hasta que haya pasado la fecha de retención. IBM Spectrum Protect para retención de datos combinado con la reclamación de volúmenes WORM FILE garantiza la protección durante el ciclo de vida de los datos.

Las agrupaciones de almacenamiento pueden gestionarse por el umbral o por el periodo de retención de datos. El parámetro de agrupación de almacenamiento RECLAMATIONTYPE indica que una agrupación de almacenamiento está gestionada en función del periodo de retención de datos. Al realizar una consulta a una agrupación de almacenamiento tradicional con el parámetro FORMAT=DETAILED, se muestra la siguiente salida:

```
Tipo de reclamación: THRESHOLD
```

Si un servidor de IBM Spectrum Protect tiene habilitada la protección de retención de datos a través de IBM Spectrum Protect para retención de datos, y el servidor tiene acceso a un archivador NetApp con la característica con licencia SnapLock, puede definir una agrupación de almacenamiento con el parámetro RECLAMATIONTYPE definido en SNAPLOCK. Esto significa que los datos creados en

volúmenes de esta agrupación de almacenamiento se gestionan por una fecha de retención. Al realizar una consulta a una agrupación de almacenamiento SnapLock con el parámetro `FORMAT=DETAILED`, la salida indica que las agrupaciones de almacenamiento están gestionadas por el periodo de retención de datos:

Tipo de reclamación: `SNAPLOCK`

Para obtener más información sobre el archivador SnapLock, consulte la documentación de NetApp *Data ONTAP Archive and Compliance Management Guide for 7-Mode*.

Atención: No utilice esta característica para proteger los datos con un periodo de retención inferior a tres meses.

- **Reclamación y la característica SnapLock**
Para garantizar la protección continua de los datos, establezca el periodo de retención predeterminado de NetApp en 30 días para que coincida con el periodo de reclamación predeterminado del volumen WORM FILE. IBM Spectrum Protect reclama todos los datos restantes en un volumen WORM FILE justo antes de la caducidad de la fecha de retención.
- **Periodos de retención**
Las políticas de IBM Spectrum Protect gestionan el periodo de retención del volumen WORM FILE. La retención de algunos archivos puede exceder el periodo de retención para el volumen WORM FILE en el que se han almacenado. Es posible que tenga que mover algunos archivos a otro volumen para garantizar que los archivos se almacenen en medios WORM.
- **Configuración de la característica SnapLock para la retención basada en sucesos**
Los datos almacenados en volúmenes SnapLock gestionados por IBM Spectrum Protect para retención de datos y la retención basada en sucesos pueden provocar una reclamación excesiva, lo que causará una disminución en el rendimiento del servidor.
- **Protección de datos continua con la característica SnapLock**
Si los datos se almacenan en un volumen con la característica SnapLock habilitada, y los datos se mueven o copian a un volumen que no sea SnapLock, los datos pierden la protección exclusiva por hardware que proporcionan los volúmenes NetApp WORM.
- **Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect**
Para cumplir los estrictos requisitos de los datos archivados, habilite la característica NetApp SnapLock.

Reclamación y la característica SnapLock

Para garantizar la protección continua de los datos, establezca el periodo de retención predeterminado de NetApp en 30 días para que coincida con el periodo de reclamación predeterminado del volumen WORM FILE. IBM Spectrum Protect reclama todos los datos restantes en un volumen WORM FILE justo antes de la caducidad de la fecha de retención.

La reclamación de un volumen WORM FILE a otro volumen WORM FILE antes de la caducidad de la fecha de retención garantiza que los datos siempre estarán protegidos por la función SnapLock.

Puesto que esta protección se realiza en el nivel de volumen de IBM Spectrum Protect, los datos de los volúmenes pueden ser gestionados por la política de IBM Spectrum Protect independientemente de dónde están almacenados los datos. Los datos almacenados en volúmenes WORM FILE están protegidos tanto por la protección de retención de datos como por el periodo de retención almacenado con el archivo físico en el volumen SnapLock. Si un administrador de IBM Spectrum Protect emite un mandato para suprimir los datos, el mandato falla. Si alguien intenta suprimir el archivo a través de una serie de llamadas del sistema de archivos de red, la función SnapLock impedirá la supresión de los datos.

Durante el proceso de reclamación, si el servidor de IBM Spectrum Protect no puede traspasar datos de un volumen SnapLock a punto de caducar a un nuevo volumen SnapLock, se mostrará un mensaje de aviso.

Periodos de retención

Las políticas de IBM Spectrum Protect gestionan el periodo de retención del volumen WORM FILE. La retención de algunos archivos puede exceder el periodo de retención para el volumen WORM FILE en el que se han almacenado. Es posible que tenga que mover algunos archivos a otro volumen para garantizar que los archivos se almacenen en medios WORM.

Es posible que algunos objetos del volumen se retengan durante más tiempo que otros objetos del volumen por los motivos siguientes:

- Los objetos están vinculados con clases de gestión con distintos periodos de retención.
- Los objetos no pueden eliminarse debido a una espera de supresión.
- Los objetos están esperando que se produzca un suceso antes de caducar.
- El periodo de retención de un grupo de copia se incrementa, lo que requiere un periodo de retención más largo que el especificado en la función SnapLock al confirmar el volumen WORM FILE.

Para gestionar un volumen WORM FILE por tiempo de retención, debe emitir el mandato `DEFINE STGPOOL` y especificar `RECLAMATIONTYPE=SNAPLOCK`. De esta forma, puede definir una agrupación de almacenamiento como una agrupación de almacenamiento SnapLock. Después, no puede actualizar el parámetro `RECLAMATIONTYPE` a un valor de `THRESHOLD`. Al definir una agrupación de almacenamiento SnapLock, el sistema verifica que los directorios especificados que están en la clase de dispositivo

estén en volúmenes SnapLock WORM. Al definir una clase de archivo y crear agrupaciones de almacenamiento con el tipo de reclamación de SNAPLOCK, todos los volúmenes deben ser volúmenes WORM para que la operación se ejecute correctamente. Si se actualiza una clase de dispositivo para que contenga directorios adicionales y se asignan agrupaciones de almacenamiento SnapLock, se realiza la misma comprobación para garantizar que todos los directorios sean volúmenes WORM SnapLock.

Hay tres periodos de retención disponibles para la característica NetApp SnapLock. Los periodos de retención deben estar configurados correctamente para que el servidor de IBM Spectrum Protect pueda gestionar correctamente los datos WORM almacenados en los volúmenes SnapLock. El servidor de IBM Spectrum Protect define el periodo de retención para los datos que se almacenan en los volúmenes SnapLock de NetApp en función de los valores del grupo de copias para los datos que se archivan. El servidor de archivos NetApp no debería entrar en conflicto con la capacidad del servidor de IBM Spectrum Protect para definir el periodo de retención. El método preferido consiste en configurar los siguientes valores para periodos de retención en el servidor de archivos NetApp:

- Periodo de retención mínimo. Defina el valor más alto: entre 30 días o el número mínimo de días especificado por cualquier grupo de copias (utilizando un servidor de archivos SnapLock de NetApp para el almacenamiento WORM FILE) para el periodo de retención de datos. El grupo de copias es el que se utiliza para almacenar datos en los volúmenes SnapLock de NetApp.
- Periodo de retención máximo. Acepte el valor predeterminado de 30 años. Este periodo de retención permite al servidor de IBM Spectrum Protect establecer el periodo de retención real del volumen en función de los valores del grupo de copia archivada.
- Periodo de retención predeterminado. Se establece en 30 días. Si no establece este valor ni el periodo máximo de retención, el periodo de retención de cada volumen se establecerá en 30 años. En este caso, el servidor de IBM Spectrum Protect no puede gestionar la caducidad y reutiliza los volúmenes NetApp SnapLock. Como resultado, no se puede reutilizar ningún volumen en 30 años.

Con los periodos de retención de SnapLock de NetApp definidos, IBM Spectrum Protect puede gestionar los datos de las agrupaciones de almacenamiento SnapLock con la máxima eficacia. IBM Spectrum Protect crea un periodo de reclamación para cada volumen que se encuentra en una agrupación de almacenamiento SNAPLOCK. El periodo de reclamación de IBM Spectrum Protect tiene una fecha de inicio, BEGIN RECLAIM PERIOD, y una fecha de finalización END RECLAIM PERIOD. Puede ver estas fechas ejecutando el mandato QUERY VOLUME con el parámetro FORMAT=DETAILED en un volumen SnapLock. La salida es similar a este ejemplo:

```
Begin Reclaim Period: 09/05/2017
End Reclaim Period: 10/06/2017
```

Cuando IBM Spectrum Protect archiva archivos en un volumen SnapLock, realiza el seguimiento de la fecha de caducidad más lejana de estos archivos y el valor de BEGIN RECLAIM PERIOD se establece en esa fecha de caducidad más lejana. Cuando se agregan más archivos al volumen SnapLock, la fecha de inicio se establece en esa fecha más reciente si existe un archivo con una fecha de caducidad posterior a la que tiene actualmente el volumen. La fecha de inicio se establece en la fecha de caducidad más lejana de cualquier archivo de ese volumen. Se espera que todos los archivos de ese volumen ya deberían haber caducado o que deberían caducar ese día. Al día siguiente, en el volumen no queda ningún dato válido.

El parámetro END RECLAIM PERIOD se define en un mes después que la fecha de BEGIN RECLAIM PERIOD. La fecha de retención establecida en el servidor de archivos NetApp para ese volumen se define en la fecha END RECLAIM PERIOD. El servidor de archivos NetApp impide la supresión de ese volumen hasta que se llegue a la fecha de END RECLAIM PERIOD. Esta fecha es aproximadamente un mes después de la caducidad de los datos en el servidor de IBM Spectrum Protect. Cuando el servidor de IBM Spectrum Protect calcula una fecha de END RECLAIM PERIOD para el volumen, y la fecha es posterior a END RECLAIM PERIOD, la fecha se restablece en el servidor de archivos NetApp para dicho volumen a una fecha posterior. Restablecer los datos a una fecha posterior garantiza que el volumen IBM Spectrum Protect WORM FILE no se suprimirá hasta que los datos del volumen hayan caducado o hasta que los datos se hayan traspasado a otro volumen SnapLock.

El periodo de reclamación de IBM Spectrum Protect es el periodo de tiempo entre la fecha de inicio y la fecha final. Durante el periodo de reclamación, el servidor de IBM Spectrum Protect suprime los volúmenes en los que todos los datos han caducado, o debe traspasar los archivos que todavía no han caducado de volúmenes SnapLock caducados a nuevos volúmenes SnapLock con nuevas fechas. Este mes resulta de gran importancia en cuanto a la seguridad y eficacia con las que el servidor gestiona los datos de volúmenes WORM FILE. Normalmente, los datos de un volumen SnapLock ya han caducado cuando llega la fecha de inicio y el volumen debería estar vacío. Al llegar la fecha final, el volumen puede suprimirse con seguridad del inventario de IBM Spectrum Protect y del servidor de archivos SnapLock.

Sin embargo, algunos sucesos pueden provocar que haya datos válidos en un volumen SnapLock:

- Es posible que el proceso de la caducidad del servidor de IBM Spectrum Protect para ese volumen se haya pospuesto o no haya finalizado.
- Es posible que los parámetros de retención del grupo de copia o de las clases de gestión asociadas se hayan alterado para un archivo después de haberse archivado, y ese archivo no caducará hasta transcurrir un cierto periodo de tiempo.
- Es posible que se haya aplicado una espera de supresión a uno o más archivos del volumen.
- El proceso de reclamación se ha inhabilitado o ha encontrado errores al traspasar datos a los nuevos volúmenes SnapLock de una agrupación de almacenamiento SnapLock.
- Un archivo está esperando que se produzca un suceso para que el servidor de IBM Spectrum Protect pueda iniciar el proceso de caducidad del archivo.

Cuando llega la fecha de inicio y los archivos en un volumen SnapLock no han caducado, los archivos deben traspasarse a un nuevo volumen SnapLock con nuevas fechas de inicio y final. Sin embargo, si se retrasa el procesamiento de la caducidad en el servidor de IBM Spectrum Protect, y dichos archivos caducan cuando se ejecuta el procesamiento de la caducidad en el servidor de IBM Spectrum Protect, no resulta eficaz traspasar esos archivos a un nuevo volumen SnapLock. Para asegurarse de que no se produce ese traspaso de datos innecesario en los archivos que están a punto de caducar, el traspaso de archivos de los volúmenes SnapLock que caducan se pospondrá hasta pasados unos días después de la fecha de BEGIN RECLAIM PERIOD date. Puesto que los datos están protegidos en el archivador SnapLock hasta la fecha de END RECLAIM PERIOD, no representa ningún riesgo posponer este traspaso de los datos. Esto permite que finalice el proceso de caducidad de IBM Spectrum Protect. Después de ese número de días, si todavía existen datos válidos en un volumen SnapLock que caduca, éstos se traspasarán a un nuevo volumen SnapLock, con lo que los datos siguen estando protegidos.

Puesto que los datos inicialmente estaban archivados, es posible que se hayan producido cambios en los parámetros de retención de los mismos (por ejemplo, en la clase de gestión o en los parámetros de agrupación de copia) o es posible que se haya aplicado una espera de supresión a esos datos. Sin embargo, los datos de ese volumen solo estarán protegidos por SnapLock hasta la fecha de END RECLAIM PERIOD. Los datos que no hayan caducado se traspasan a nuevos volúmenes SnapLock durante el periodo de reclamación de IBM Spectrum Protect. Si se producen errores al traspasar los datos a un nuevo volumen SnapLock, se emite un mensaje de aviso que indica que los datos pronto dejarán de estar protegidos. Si el error persiste, emita el mandato MOVE DATA para el volumen con problemas.

Atención: No inhabilite el proceso de reclamación de una agrupación de almacenamiento SnapLock. Una vez inhabilitado el proceso, el servidor de IBM Spectrum Protect no tiene forma de mostrar los mensajes de aviso de que los datos dejarán de estar protegidos. Esta situación también puede producirse si se inhabilitan la reclamación y migración para todo el servidor (por ejemplo, si se ha establecido NOMIGRRECL en el archivo de opciones del servidor). Asegúrese de que los datos estén protegidos al gestionar las agrupaciones de almacenamiento SnapLock.

Configuración de la característica SnapLock para la retención basada en sucesos

Los datos almacenados en volúmenes SnapLock gestionados por IBM Spectrum Protect para retención de datos y la retención basada en sucesos pueden provocar una reclamación excesiva, lo que causará una disminución en el rendimiento del servidor.

Si los datos se gestionan mediante la retención basada en sucesos, IBM Spectrum Protect establece inicialmente el periodo de retención en el valor más grande de los valores RETVER y RETMIN para el grupo de copias archivadas. Cuando el volumen entra en el periodo de reclamación y los datos que permanecen en el volumen se trasladan, el periodo de retención del volumen de destino se establece en el periodo de retención restante de los datos, que normalmente es 0. El nuevo volumen entrará en el periodo de reclamación poco de recibir los datos, lo que provocará la reclamación de volúmenes que se acababan de crear.

Puede evitar esta situación utilizando la opción de servidor RETENTIONEXTENSION. Esta opción permite al servidor establecer o ampliar la fecha de retención de un volumen SnapLock. Puede especificar un valor en el rango de 30 - 9999 días. El valor predeterminado es 365 días.

Al seleccionar volúmenes de una agrupación de almacenamiento SnapLock para la reclamación, el servidor comprueba si el volumen está dentro del periodo de reclamación:

- Si el volumen no está dentro del periodo de retención, no se realiza ninguna acción. El volumen no se reclama y la fecha de retención no se modifica.
- Si el volumen está dentro del periodo de reclamación, el servidor comprueba si el porcentaje de espacio reclamable del volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento o del porcentaje de umbral pasado en el parámetro THRESHOLD de un mandato RECLAIM STGPOOL:
 - Si el espacio reclamable es mayor que el umbral, el servidor reclama el volumen y define la fecha de retención del volumen de destino en el valor mayor de los siguientes:
 - El periodo de retención restante de los datos más 30 días para el periodo de reclamación.
 - El valor RETENTIONEXTENSION más 30 días para el periodo de reclamación.
 - Si el espacio reclamable no es mayor que el umbral, el servidor restablece la fecha de retención del volumen según la cantidad especificada en la opción RETENTIONEXTENSION. El nuevo periodo de retención se calcula agregando el número de días especificado a la fecha actual.

En los ejemplos descritos a continuación, el volumen SnapLock, VolumeA, está en una agrupación de almacenamiento cuyo umbral de reclamación se establece en 60%. La opción de servidor RETENTIONEXTENSION se define en 365 días. El periodo de retención para VolumeA está en el periodo de reclamación. En las siguientes situaciones se muestra cómo queda afectada la retención:

- El espacio reclamable en VolumeA es inferior al 60%. La fecha de retención de VolumeA se amplía en 365 días.
- El espacio reclamable en VolumeA es superior al 60%, y el periodo de retención restante de los datos es superior a 365 días. VolumeA se reclama, y la fecha de retención del volumen de destino se define en el periodo de retención restante de los datos más 30 días para el periodo de reclamación.

- El espacio reclamable en VolumeA es superior al 60%, y el periodo de retención de los datos es inferior a 365 días. VolumeA se reclama y su fecha de retención se define en 365 días, el valor RETENTIONEXTENSION más 30 días para el periodo de reclamación.

Protección de datos continua con la característica SnapLock

Si los datos se almacenan en un volumen con la característica SnapLock habilitada, y los datos se mueven o copian a un volumen que no sea SnapLock, los datos pierden la protección exclusiva por hardware que proporcionan los volúmenes NetApp WORM.

El servidor de IBM Spectrum Protect permite este tipo de movimiento. Sin embargo, si los datos se mueven de un volumen WORM FILE a otro tipo de medio, puede que los datos dejen de estar protegidos contra la supresión por error o intencionada. Si estos datos se encuentran en volúmenes WORM para cumplir los requisitos de retención y protección de datos para finalidades de condiciones de uso y se traspan a otro medio, puede que los datos dejen de cumplir dichos requisitos. Debe configurar sus agrupaciones de almacenamiento de forma que este tipo de datos se mantenga en las agrupaciones de almacenamiento formadas por volúmenes WORM SnapLock durante todo el periodo de retención de datos.

Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect

Para cumplir los estrictos requisitos de los datos archivados, habilite la característica NetApp SnapLock.

Acerca de esta tarea

Al definir o actualizar configuraciones que incluyen agrupaciones de almacenamiento SnapLock, asegúrese de que la opción RECLAMATIONTYPE=SNAPLOCK esté especificada para las agrupaciones de almacenamiento seleccionadas para los parámetros NEXTSTGPOOL, RECLAIMSTGPOOL y COPYSTGPOOLS.

Si configura las agrupaciones de almacenamiento de esta manera, ayuda a asegurar la protección de sus datos. Si define una agrupación de almacenamiento siguiente, de reclamación, de copia o de datos activos sin seleccionar la opción RECLAMATIONTYPE=SNAPLOCK, la agrupación de almacenamiento no está protegida. El mandato se ejecuta correctamente, pero se emite un mensaje de error.

Procedimiento

Para configurar un volumen SnapLock para utilizar como un volumen IBM Spectrum Protect WORM FILE, complete los siguientes pasos:

1. Instale y configure SnapLock en el servidor de archivos NetApp. Asegúrese de configurar correctamente los periodos de retención mínimo, máximo y predeterminado. Para obtener instrucciones, consulte la documentación de NetApp.
2. Instale y configure el servidor de IBM Spectrum Protect.
3. Habilite la protección de retención de datos de archivos emitiendo mandato SET ARCHIVERETENTIONPROTECTION:

```
set archiveretentionprotection on
```
4. Configure la política mediante el mandato DEFINE COPYGROUP. Seleccione los valores RETVER y RETMIN en el grupo de copias archivadas que cumpla sus requisitos de protección de datos del almacenamiento WORM. Si no se especifican los valores RETVER ni RETMIN, se utilizan los valores de clases de gestión predeterminados.
5. Configure el almacenamiento mediante el mandato DEFINE DEVCLASS.
 - Utilice la clase de dispositivo FILE.
 - Especifique el parámetro DIRECTORY para que apunte al directorio o directorios de los volúmenes SnapLock.
6. Defina una agrupación de almacenamiento utilizando la clase de dispositivo que se define en el paso 5 emitiendo el mandato DEFINE STGPOOL y especifique el parámetro RECLAMATIONTYPE=SNAPLOCK.
7. Actualice el grupo de copias para que señale a la agrupación de almacenamiento emitiendo el mandato UPDATE COPYGROUP.
8. Utilice la API (interfaz de programación de aplicaciones) de IBM Spectrum Protect para archivar sus objetos en la agrupación de almacenamiento de SnapLock. Esta función no está disponible en los clientes de copia de seguridad/archivado de IBM Spectrum Protect estándar.

Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedores de directorios

Puede reparar extensiones de datos dañados en agrupaciones de almacenamiento de contenedores de directorios y recuperar datos perdidos después de un siniestro.

Las extensiones de datos forman parte de un archivo que se crea durante el proceso de eliminación de duplicados de datos. Las extensiones se comparan con otras extensiones de archivo para identificar los duplicados. Si su agrupación de almacenamiento de contenedores de directorio tiene archivos o directorios dañados, puede reparar las extensiones de datos con duplicados eliminados desde el servidor de réplica de destino, el servidor de réplica de origen o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.

- **Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino**
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen desde el servidor de réplica de destino.
- **Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor**
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedor de directorios en el servidor de origen recuperando las extensiones de datos deduplicados de los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor del local o de fuera del local.
- **Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor**
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.
- **Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino**
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de destino, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de origen.
- **Reparación de agrupaciones de almacenamiento después de un siniestro**
Puede reparar las agrupaciones de almacenamiento de contenedores de directorio y recuperar los datos perdidos después de un siniestro.
- **Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado**
Si se daña un volumen de cinta que almacena una copia de las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de copia de contenedor, puede sustituir el volumen.

Conceptos relacionados:

Estrategias para la protección ante siniestro

Tareas relacionadas:

Soluciones de protección de datos

Recuperación de pérdida de datos o de paradas del sistema

Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen desde el servidor de réplica de destino.

Antes de empezar

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Asegúrese de que exista espacio suficiente en la agrupación de almacenamiento de contenedores de directorio para los datos recuperados. El parámetro `PREVIEW=YES` del mandato `REPAIR STGPOOL` especifica la cantidad de datos que se repararán. Si no hay espacio suficiente, utilice el mandato `DEFINE STGPOOLDIRECTORY` para proporcionar espacio.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.

- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados se reparan con las extensiones que se han protegido en el servidor de réplica de destino. Restricción: Puede emitir el mandato REPAIR STGPOOL para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en otra agrupación de almacenamiento de un servidor de réplica de destino mediante el mandato PROTECT STGPOOL.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Procedimiento

1. Si sospecha que existen daños menores, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores en el nivel de directorio, de modo que pueda identificar las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio. Si identifica las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar. Para ahorrar tiempo y recursos, únicamente realice la auditoría de los contenedores que sospecha que están dañados. Si cree que su agrupación de almacenamiento de contenedores de directorio presenta un daño más grave, emita el mandato AUDIT CONTAINER en el nivel de la agrupación de almacenamiento.

Por ejemplo, para realizar la auditoría de un directorio, n:\pooldir, de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1 stgpooledirectory=n:\pooldir
```

Para realizar una auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Es posible que el proceso de auditoría tarde varias horas.

2. Para reparar una agrupación de almacenamiento de contenedores de directorio, emita el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER. Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

3. Identifique cualquier extensión dañada adicional con el mandato QUERY DAMAGED.
4. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:
 - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
 - b. Si un directorio de agrupación de almacenamiento completo está dañado, cree un nuevo directorio de agrupación de almacenamiento de sustitución mediante el mandato DEFINE STGPOOLDIRECTORY.
 - c. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

- d. Opcionalmente, emita el mandato DELETE STGPOOLDIRECTORY para suprimir el directorio de la agrupación de almacenamiento vacío que ha sustituido por un nuevo directorio en el paso 4.b.

Qué hacer a continuación

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)

REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)

DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedor de directorios en el servidor de origen recuperando las extensiones de datos deduplicados de los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor del local o de fuera del local.

Antes de empezar

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Asegúrese de que exista espacio suficiente en la agrupación de almacenamiento de contenedores de directorio para los datos recuperados. El parámetro PREVIEW=YES del mandato REPAIR STGPOOL especifica la cantidad de datos que se repararán. Si no hay espacio suficiente, utilice el mandato DEFINE STGPOOLDIRECTORY para proporcionar espacio.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados se reparan con las extensiones que se han protegido en las agrupaciones de almacenamiento de copia de contenedor.

Restricción: Puede emitir el mandato REPAIR STGPOOL para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en las agrupaciones de almacenamiento de copia de contenedor mediante el mandato PROTECT STGPOOL.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

Procedimiento

1. Si sospecha que existen daños menores, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores en el nivel de directorio, de modo que pueda identificar las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio. Si identifica las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar. Para ahorrar tiempo y recursos, únicamente realice la auditoría de los contenedores que sospecha que están dañados. Si cree que su agrupación de almacenamiento de contenedores presenta un daño más grave, emita el mandato AUDIT CONTAINER en el nivel de la agrupación de almacenamiento. Por ejemplo, para realizar la auditoría de un directorio, n:\pooldir, de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
```

Para realizar una auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```


Es posible que el proceso de auditoría tarde varias horas.

Durante la operación de reparación, el servidor le solicita los volúmenes que necesita. En el paso 3, traerá los volúmenes al local y los comprobará en la biblioteca. Los volúmenes necesarios se deben llevar al local y comprobar en la biblioteca.

2. Para obtener una vista previa de la operación de reparación y generar la lista de los volúmenes de cinta necesarios para la operación, emita el mandato REPAIR STGPOOL y especifique los parámetros SRCLOCATION=LOCAL y PREVIEW=YES. Por ejemplo, para obtener la vista previa de la operación de reparación de una agrupación de almacenamiento con el nombre STGPOOL1 de las agrupaciones de almacenamiento de copia de contenedor, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local preview=yes
```

Es posible que el proceso de vista previa tarde algún tiempo en finalizar.

3. Si algunos de los volúmenes necesarios están fuera del local, realice los pasos siguientes:
 - a. Utilice la lista de la operación de vista previa para determinar qué volúmenes deben regresar al local.
 - b. Cuando los volúmenes estén en el local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE.
 - c. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.

Para obtener instrucciones detalladas sobre la función del gestor de recuperación ante siniestro (DRM), consulte Utilización del gestor de recuperación ante siniestro para entornos de cinta (V7.1.1).

4. En función de la información que obtenga durante la operación de vista previa, asegúrese de que la agrupación de almacenamiento tiene espacio suficiente para los datos recuperados. Si no hay espacio suficiente, utilice el mandato DEFINE STGPOOLDIRECTORY para proporcionar espacio.
5. Para reparar la agrupación de almacenamiento de contenedores de directorio, emita el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=LOCAL.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde una agrupación de almacenamiento de copia de contenedor, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

6. Identifique cualquier extensión dañada adicional con el mandato QUERY DAMAGED.
7. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde las agrupaciones de almacenamiento de copia de contenedor, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:
 - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
 - b. Si un directorio de agrupación de almacenamiento completo está dañado, cree un nuevo directorio de agrupación de almacenamiento de sustitución mediante el mandato DEFINE STGPOOLDIRECTORY.
 - c. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

- d. Opcionalmente, emita el mandato DELETE STGPOOLDIRECTORY para suprimir el directorio de la agrupación de almacenamiento vacío que ha sustituido por un nuevo directorio en el paso 7.b.
8. Si ha reparado un directorio de agrupación de almacenamiento completo, suprima el directorio original, que está vacío y se ha sustituido por un nuevo directorio. Suprima el directorio original emitiendo el mandato DELETE STGPOOLDIRECTORY.

Qué hacer a continuación

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)
DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.

Antes de empezar

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Asegúrese de que exista espacio suficiente en la agrupación de almacenamiento de contenedores de directorio para los datos recuperados. El parámetro PREVIEW=YES del mandato REPAIR STGPOOL especifica la cantidad de datos que se repararán. Si no hay espacio suficiente, utilice el mandato DEFINE STGPOOLDIRECTORY para proporcionar espacio.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones que se han protegido en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor de un servidor de origen.

Restricción: Puede emitir el mandato REPAIR STGPOOL para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en otra agrupación de almacenamiento de un servidor de réplica de destino, o en agrupaciones de almacenamiento de copia de contenedor, mediante el mandato PROTECT STGPOOL.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

Procedimiento

1. Intente reparar la agrupación de almacenamiento desde el servidor de réplica realizando los pasos de la sección Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino.
2. Si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino, repare las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor realizando los pasos de la sección Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor.
3. Si ha reparado las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor, emita el mandato PROTECT STGPOOL y especifique el parámetro TYPE=REPLSERVER para las agrupaciones de almacenamiento del servidor de réplica de origen.

Qué hacer a continuación

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato `AUDIT CONTAINER` para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre `STGPOOL1`, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Referencia relacionada:

`AUDIT CONTAINER` (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

`DEFINE SCHEDULE` (Definir una planificación para un mandato de administración)

`QUERY DAMAGED` (Consultar los datos de la agrupación de almacenamiento dañada)

`PROTECT STGPOOL` (Protección de datos de agrupación de almacenamiento)

`REPAIR STGPOOL` (Reparar una agrupación de almacenamiento de contenedores de directorio)

`DEFINE STGPOOLDIRECTORY` (Definir un directorio de agrupaciones de almacenamiento)

`DELETE STGPOOLDIRECTORY` (Suprimir un directorio de agrupación de almacenamiento)

Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de destino, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de origen.

Antes de empezar

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Como parte de la operación del mandato `PROTECT STGPOOL`, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato `AUDIT CONTAINER` podría identificar daños en la agrupación de almacenamiento de destino antes de que se emita el mandato `PROTECT STGPOOL`.

Procedimiento

1. Proteja las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en un servidor de origen emitiendo el mandato `PROTECT STGPOOL`.

Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio con el nombre `POOL1`, emita el siguiente mandato:

```
protect stgpool pool1
```

Espere a que finalice el proceso de protección.

2. Para identificar las extensiones de datos dañadas que se encuentran en la agrupación de almacenamiento de contenedores de directorio del servidor de destino, emita el mandato `AUDIT CONTAINER`.

Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre `STGPOOL1`, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

3. Repare las extensiones dañadas en la agrupación de almacenamiento de destino emitiendo de nuevo el mandato `PROTECT STGPOOL` en el servidor de origen. Las extensiones dañadas en la agrupación de almacenamiento de destino se marcarán como

dañadas y se repararán.

4. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.

Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)

REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)

DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

Reparación de agrupaciones de almacenamiento después de un siniestro

Puede reparar las agrupaciones de almacenamiento de contenedores de directorio y recuperar los datos perdidos después de un siniestro.

En caso de siniestro, si su sitio primario ya no está disponible, puede reparar sus agrupaciones de almacenamiento de contenedores de directorio restaurándolas en un nuevo servidor de destino de su sitio de recuperación.

- Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro
Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.
- Reparación de agrupaciones de almacenamiento desde un servidor de réplica después de un siniestro
Si se produce un siniestro en un servidor de réplica, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.
- Reparación de las agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.
Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

Referencia relacionada:

Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro

Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de origen
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Está utilizando el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local desde un servidor de origen. Ha recuperado los volúmenes de cinta de fuera del local y los tiene en su sitio de recuperación.
- No ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en un servidor de réplica de destino.

- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dsmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

Procedimiento

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Si ha protegido la agrupación de almacenamiento de contenedores de directorio utilizando las agrupaciones de almacenamiento de copia de contenedor en el local y fuera del local, emita el mandato UPDATE STGPOOL para la copia del local de las agrupaciones de almacenamiento de copia de contenedor y especifique el parámetro ACCESS=UNAVAILABLE.
3. Cuando los volúmenes de la agrupación de almacenamiento de copia de contenedor de fuera del local regresen al local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE.
4. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.
5. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=LOCAL.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde agrupaciones de almacenamiento de copia de contenedor de fuera del local, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

6. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
7. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

Reparación de agrupaciones de almacenamiento desde un servidor de réplica después de un siniestro

Si se produce un siniestro en un servidor de réplica, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de réplica
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos desde un servidor de réplica de origen a un servidor de réplica de destino. El servidor de réplica de destino se ejecuta en su sitio de recuperación.
- No ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local.

- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dsmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Procedimiento

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica de destino, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDLAY.

3. Si no ha utilizado scripts de configuración Blueprint para configurar el servidor de réplica de destino, es posible la estructura de archivos del servidor de réplica de destino no coincida con la información almacenada en la base de datos. Opcionalmente, elimine los directorios de la agrupación de almacenamiento que no existan en el servidor de réplica de destino, emitiendo el mandato DELETE STGPOOLDIRECTORY.
4. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
5. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:
 - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
 - b. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

6. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

Referencia relacionada:

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

Reparación de las agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.

Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

Acerca de esta tarea

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de origen
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos desde un servidor de réplica de origen a un servidor de réplica de destino. El servidor de réplica de destino se ejecuta en su sitio de recuperación.
- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local.
- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

Procedimiento

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Si ha protegido la agrupación de almacenamiento de contenedores de directorio utilizando las agrupaciones de almacenamiento de copia de contenedor en el local y fuera del local, emita el mandato UPDATE STGPOOL para la copia del local de las agrupaciones de almacenamiento de copia de contenedor y especifique el parámetro ACCESS=UNAVAILABLE.
3. Cuando los volúmenes de la agrupación de almacenamiento de copia de contenedor de fuera del local regresen al local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE. Si ahora traslada los volúmenes de cinta al local, estará preparado para reparar las extensiones dañadas de los volúmenes de cinta de copia de contenedor, si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino.
4. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.
5. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica de destino, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDelay.

6. Si no ha utilizado scripts de configuración Blueprint para configurar el servidor de réplica de destino, es posible la estructura de archivos del servidor de réplica de destino no coincida con la información almacenada en la base de datos. Opcionalmente, elimine los directorios de la agrupación de almacenamiento que no existan en el servidor de réplica de destino. Emita el mandato DELETE STGPOOLDIRECTORY para suprimir los directorios que no estén en el servidor de réplica de destino.

7. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
8. Si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino, puede reparar las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor de fuera del local. Para obtener las instrucciones, consulte Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.
9. Confirme que no existen extensiones dañadas adicionales volviendo a emitir el mandato QUERY DAMAGED.
10. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad. Después de los dos ciclos de copia de seguridad, realice estos pasos:
 - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
 - b. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

11. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado

Si se daña un volumen de cinta que almacena una copia de las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de copia de contenedor, puede sustituir el volumen.

Procedimiento

1. Suprime el volumen de cinta dañado emitiendo el mandato DELETE VOLUME y especificando el parámetro DISCARDATA=YES. Por ejemplo, para suprimir un volumen con el nombre VOLUME1, emita el siguiente mandato:

```
delete volume volume1 discarddata=yes
```

2. Puede proteger las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio copiando los datos en los volúmenes existentes de una agrupación de almacenamiento de copia de contenedor. Emita el mandato PROTECT STGPOOL desde el servidor de origen.
Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio con el nombre POOL1, emita el siguiente mandato:

```
protect stgpool pool1 type=local
```

Referencia relacionada:

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)
DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

Mandatos, opciones y programas de utilidad del servidor

Utilice mandatos para administrar y configurar el servidor, opciones para personalizar el servidor y los programas de utilidad para realizar tareas especiales cuando el servidor no se está ejecutando.

- Gestión del servidor desde la línea de mandatos
IBM Spectrum Protect proporciona varias interfaces de línea de mandatos diferentes para gestionar servidores de IBM Spectrum Protect.
- Mandatos de administración
Los mandatos de administración están disponibles para gestionar y configurar el servidor.
- Opciones de servidor
Durante la instalación, IBM Spectrum Protect proporciona un archivo de opciones de servidor que contiene un conjunto de opciones predeterminadas para iniciar el servidor.
- Herramientas del servidor
Utilice las herramientas del servidor para realizar tareas especiales en el servidor mientras éste no está en ejecución.
- Códigos de retorno de los scripts para IBM Spectrum Protect
Puede escribir scripts de IBM Spectrum Protect que utilizan códigos de retorno para determinar cómo continúa el proceso de script. Los códigos de retorno pueden ser de una de estas tres gravedades: OK, WARNING, ERROR.

- Programas de utilidad de dispositivos
Puede utilizar programas de utilidad de dispositivos para las tareas que están relacionadas con la configuración de dispositivos de almacenamiento para el servidor de IBM Spectrum Protect.
- Scripts del servidor y macros para la automatización
Puede automatizar las tareas administrativas más comunes creando scripts del servidor de IBM Spectrum Protect o macros del cliente administrativo. Los scripts del servidor se almacenan en la base de datos del servidor y pueden planificarse para ejecutarse con un mandato de planificación de administración. Las macros del cliente administrativo se almacenan como archivos en el cliente administrativo.

Gestión del servidor desde la línea de mandatos

IBM Spectrum Protect proporciona varias interfaces de línea de mandatos diferentes para gestionar servidores de IBM Spectrum Protect.

Acerca de esta tarea

Están disponibles las interfaces de línea de mandatos siguientes:

Cliente de línea de mandatos de administración

El cliente de línea de mandatos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal. Se instala como parte del proceso de instalación del servidor de IBM Spectrum Protect. Se puede acceder al cliente de administración remotamente.

En el cliente de administración, puede emitir cualquier mandato de servidor.

Consola del servidor

La consola del servidor es una ventana de línea de mandatos en el sistema en el que está instalado el servidor. Por consiguiente, para utilizar la consola del servidor, debe encontrarse en la ubicación física del sistema servidor.

En comparación con el cliente de administración, las capacidades de la consola del servidor son limitadas. Desde la consola del servidor, no puede emitir determinados mandatos y no puede direccionar mandatos a otros servidores. Además, no puede especificar que determinados mandatos se procesen antes de que puedan emitirse otros mandatos. No obstante, esta limitación puede ser útil si, por ejemplo, desea ejecutar dos mandatos en sucesión rápida.

Línea de mandatos de Centro de operaciones

En el Centro de operaciones, puede acceder a la línea de mandatos de IBM Spectrum Protect. Puede que desee utilizar esta línea de mandatos para emitir mandatos del servidor y completar determinadas tareas de IBM Spectrum Protect que no están soportadas en el Centro de operaciones.

Los scripts de servidor proporcionan la automatización de las tareas administrativas comunes. Una macro es un archivo que contiene uno o varios mandatos de administración de IBM Spectrum Protect. Cuando se emite el mandato MACRO, el servidor procesa todos los mandatos del archivo de macro en orden, incluidos los mandatos que están contenidos en las macros anidadas.

- Emisión de mandatos del cliente de administración
El cliente de línea de mandatos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal.
- Emisión de mandatos desde el Centro de operaciones
En la interfaz de mandatos del Centro de operaciones, puede emitir mandatos para gestionar servidores de IBM Spectrum Protect que están configurados como servidores concentradores o de radio.
- Emisión de mandatos desde la consola del servidor
IBM Spectrum Protect proporciona un ID de usuario denominado SERVER_CONSOLE que permite emitir mandatos y administrar el servidor desde la consola del servidor después de instalar IBM Spectrum Protect. Durante la instalación, SERVER_CONSOLE se registra automáticamente como un administrador y se le otorga autorización del sistema.
- Especificación de mandatos de administración
Los mandatos se componen de nombres de mandatos y suelen contener parámetros y variables. Los diagramas de sintaxis muestran las reglas que deben seguirse al especificar mandatos.
- Control del proceso de mandatos
Puede ejecutar algunos mandatos de IBM Spectrum Protect secuencialmente o simultáneamente con otros mandatos. También puede direccionar los mandatos de un servidor a otros servidores para su proceso.
- Realización de tareas simultáneamente en varios servidores
El direccionamiento de mandatos permite direccionar los mandatos a uno o más servidores para que los procesen y, a continuación, recopilar la salida de estos servidores.
- Clases de privilegio
La autorización que se otorga a un administrador mediante la clase de privilegio determina qué mandatos de administración puede emitir el administrador.

Conceptos relacionados:

Scripts de servidor

Referencia relacionada:

Macros de cliente administrativo

Emisión de mandatos del cliente de administración

El cliente de línea de mandatos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal.

Acerca de esta tarea

Asegúrese de que su el servidor y el cliente de administración utilizan idiomas compatibles. Consulte el apartado LANGUAGE para conocer opciones de idioma y entorno regional. Si el cliente y el servidor utilizan idiomas diferentes, los mensajes que genere IBM Spectrum Protect podrían no ser comprensibles.

Consejo: Las series de texto que se envían desde el cliente al servidor no dependen del valor de idioma del servidor. El texto se muestra correctamente si el cliente administrativo se ejecuta en el mismo entorno local al enviar la serie y al recibir la serie.

Por ejemplo, suponga que actualiza un campo de contacto de nodo con un valor que contiene caracteres nacionales (`update node miNodo contact=información_contacto_NL`), y más adelante consulta el nodo (`query node miNodo format=detailed`). Si el cliente se ejecuta en el mismo entorno local cuando se actualiza y cuando se consulta, la *información_contacto_NL* se visualiza correctamente. Si actualiza el campo de contacto de nodo cuando el cliente se ejecuta en un entorno local y consulta el nodo cuando el cliente se está ejecutando en un entorno local diferente, es posible que la *información_contacto_NL* no se visualice correctamente.

- Inicio y detención del cliente de administración
Utilice el mandato DSMADMC para iniciar una sesión del cliente de administración.
- Supervisión de actividades del servidor desde el cliente de administración
Para supervisar actividades de IBM Spectrum Protect, como la migración del servidor e inicios de sesión de cliente, ejecute el cliente de administración en modalidad de consola. No puede entrar ningún mandato de administración en modalidad de consola.
- Supervisión de montajes de medios extraíbles del cliente de administración
Para supervisar el montaje y desmontaje de medios extraíbles, ejecute el cliente de administración en modalidad de montaje. Cuando el cliente se ejecuta en modalidad de montaje, no puede especificar mandatos de administración.
- Proceso de mandatos individuales desde el cliente de administración
Utilice la modalidad de proceso por lotes para especificar un solo mandato de administración. La sesión del cliente de administración finaliza automáticamente cuando se procesa el mandato.
- Proceso de una serie de mandatos del cliente de administración
Utilice la modalidad interactiva para procesar una serie de mandatos de administración.
- Formateo de la salida de los mandatos
IBM Spectrum Protect formatea la salida procesada de los mandatos según el ancho de la pantalla o de la ventana.
- Cómo guardar la salida del mandato en una ubicación especificada
El uso más común para redirigir la salida es guardar la salida de los mandatos de consulta en un archivo o programa especificado. A continuación, puede examinar el contenido del archivo o, en algunos casos, imprimir dicho contenido.
- Opciones de cliente de administración
En todas las modalidades del cliente de administración, se pueden utilizar las opciones para modificar las respuestas a la sesión del cliente de administración.

Inicio y detención del cliente de administración

Utilice el mandato DSMADMC para iniciar una sesión del cliente de administración.

Acerca de esta tarea

El servidor de IBM Spectrum Protect debe encontrarse en ejecución para que un cliente de administración pueda conectarse.

Procedimiento

- Para iniciar una sesión del cliente de administración en modalidad de línea de mandatos, especifique este mandato en la estación de trabajo.

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

Si especifica el mandato DSMADMC con las opciones -ID y -PASSWORD como se muestra, no se le solicitan un ID de usuario y una contraseña.

- Para detener una sesión de cliente de línea de mandatos administrativos, escriba el mandato siguiente:

```
quit
```

- Para interrumpir un mandato DSMADMC antes de que el servidor de IBM Spectrum Protect termine de procesarlo, utilice el mandato UNIX `kill -9` en una línea de mandatos disponible. No pulse `Control+C` porque, cuando finaliza la sesión, puede producir resultados inesperados.

Supervisión de actividades del servidor desde el cliente de administración

Para supervisar actividades de IBM Spectrum Protect, como la migración del servidor e inicios de sesión de cliente, ejecute el cliente de administración en modalidad de consola. No puede entrar ningún mandato de administración en modalidad de consola.

Procedimiento

- Para iniciar una sesión de cliente de administración en modalidad de consola, especifique el siguiente mandato:

```
dsmadmc -consolemode
```

Se le solicitará una contraseña si está activada la autenticación para el servidor. Si no desea que se le solicite el ID de usuario y la contraseña, entre el mandato DSMADMC con las opciones -ID y -PASSWORD.

- Para finalizar una sesión de cliente de administración en modalidad de consola, utilice una secuencia de interrupción de teclado.

Sistema operativo	Secuencia de interrupción
Cientes de UNIX y Linux	Control+C
Cientes de Windows	Control+C o Control+INTER

Supervisión de montajes de medios extraíbles del cliente de administración

Para supervisar el montaje y desmontaje de medios extraíbles, ejecute el cliente de administración en modalidad de montaje. Cuando el cliente se ejecuta en modalidad de montaje, no puede especificar mandatos de administración.

Procedimiento

- Para iniciar una sesión de cliente de administración en modalidad de montaje, especifique el siguiente mandato:

```
dsmadmc -mountmode
```

Se le solicitará una contraseña si está activada la autenticación para el servidor. Si no desea que se le solicite el ID de usuario y la contraseña, entre el mandato DSMADMC con las opciones -ID y -PASSWORD.

- Para finalizar una sesión de cliente de administración en modalidad de montaje, utilice una secuencia de interrupción de teclado.

Sistema operativo	Secuencia de interrupción
Cientes de UNIX y Linux	Control+C
Cientes de Windows	Control+C o Control+INTER

Proceso de mandatos individuales desde el cliente de administración


Utilice la modalidad de proceso por lotes para especificar un solo mandato de administración. La sesión del cliente de administración finaliza automáticamente cuando se procesa el mandato.

Procedimiento

Para iniciar una sesión de cliente de administración en modalidad de proceso por lotes, use el siguiente mandato `dsmadmc mandato_servidor:`

Si no desea que se le solicite el identificador de usuario y la contraseña, puede entrar el mandato DSMADMC con las opciones -ID y -PASSWORD.

En modalidad por lotes, debe entrar el mandato completo en una línea. Si un mandato no cabe en una línea, entre el mandato utilizando una macro o un script. Si especifica un parámetro con un texto utilizando la modalidad de proceso por lotes, delimite el texto entre comillas simples (' ') en la macro. No utilice comillas dobles para los mandatos en la modalidad por lotes, pues puede que el sistema operativo no analice correctamente las comillas.

 Sistemas operativos Windows Puede eludir esta restricción de las comillas dobles en la modalidad por lotes para los clientes de Windows con el carácter de escape de barra inclinada invertida (\). Por ejemplo, en el parámetro OBJECTS del mandato DEFINE CLIENTACTION, puede especificar la serie con el carácter \ delante de las comillas dobles del mandato.

```
dsmadmc -id=admin -password=admin define
clientaction test_node domain=test_dom
action=restore objects=\"C:\Archivos de programa\test\*\\"'
```

Proceso de una serie de mandatos del cliente de administración

Utilice la modalidad interactiva para procesar una serie de mandatos de administración.

Acerca de esta tarea

Para arrancar una sesión de cliente de administración en modalidad interactiva, debe haber disponible una sesión del servidor. Para garantizar la disponibilidad de las sesiones del servidor para sesiones de administración y de nodo cliente, la modalidad interactiva del cliente de administración se desconecta si se cumplen una o varias de las condiciones siguientes:

- El servidor se ha detenido utilizando el mandato HALT.
- Los mandatos no se han emitido desde la sesión de cliente de administración durante el plazo de tiempo especificado con la opción del servidor IDLETIMEOUT.
- La sesión del cliente de administración se ha cancelado con el mandato CANCEL SESSION.

Procedimiento

Para iniciar una sesión de cliente de administración en modalidad interactiva, utilice el siguiente mandato: `dsmadmc`.

Puede utilizar caracteres de continuación en la modalidad interactiva. Para obtener más información, consulte el apartado Utilización de caracteres de continuación para entrar mandatos largos.

Puede reiniciar automáticamente la sesión de cliente de administración si especifica otro mandato cada vez que aparece el indicador `tsm: nombre_servidor >`.

No especifique un mandato de servidor con el mandato DSMADMC. Si lo hace, se iniciará el cliente de administración en modo por lotes, no en modo interactivo. Por ejemplo, no especifique:

```
dsmadmc mandato_servidor
```

Formateo de la salida de los mandatos

IBM Spectrum Protect formatea la salida procesada de los mandatos según el ancho de la pantalla o de la ventana.

Procedimiento

- Si la anchura de la pantalla o ventana no es suficiente para visualizar la salida horizontalmente, IBM Spectrum Protect organiza y visualiza la información verticalmente.
- Puede formatear la salida de los mandatos QUERY utilizando las opciones del cliente de administración DISPLAYMODE y OUTFILE.

Cómo guardar la salida del mandato en una ubicación especificada

El uso más común para redirigir la salida es guardar la salida de los mandatos de consulta en un archivo o programa especificado. A continuación, puede examinar el contenido del archivo o, en algunos casos, imprimir dicho contenido.

Acerca de esta tarea

En algunos sistemas operativos, es posible redirigir la salida de un mandato si se utilizan caracteres especiales como, por ejemplo, `>`, `>>` y `|`. Los caracteres de redirección dirigen la salida de un mandato a un archivo o programa que se especifique en lugar de dirigirla a

la pantalla. Puede guardar la salida de un mandato entrando los caracteres de redirección al final del mandato. Para redirigir la salida, deje un espacio en blanco entre el carácter de redirección y el nombre del archivo o programa. Consulte los ejemplos siguientes.

Al redirigir la salida, debe seguir los convenios de denominación del sistema operativo en el que esté ejecutando el cliente administrativo.

Procedimiento

Los ejemplos de la tabla siguiente muestran cómo redirigir la salida del mandato.

Tarea	Procedimiento
Redirigir la salida del mandato QUERY DOMAIN a un nuevo archivo en modalidad interactiva o de proceso por lotes	Utilice un único signo de mayor que (>) para redirigir la salida a un nuevo archivo o grabar sobre un archivo existente: <code>dsmadm -id=xxx -pa=xxx query domain acctg > dominfo.acc</code>
Agregar la salida de un mandato QUERY DOMAIN al final de un archivo existente en modalidad de proceso por lotes o interactiva	Utilice dos signos de mayor que (>>) para añadir la salida al final de un archivo existente: <code>dsmadm -id=xxx -pa=xxx query domain acctg >> dominfo.acc</code>
Redirigir toda la salida de una sesión de cliente de administración en modalidad de consola a un programa denominado filter.exe	Utilice la barra vertical () para dirigir toda la salida de una sesión a un programa: <code>dsmadm -console -id=admin -password=xxx filter.exe</code> El programa se puede configurar para supervisar la salida de mensajes individuales a medida que se producen y realizar la acción adecuada como, por ejemplo, enviar correo a otro usuario.
En la modalidad de consola, redirigir toda la salida a un archivo	Especifique la opción -OUTFILE con el nombre de un archivo de destino. Por ejemplo, el mandato siguiente redirige toda la salida al archivo save.out: <code>dsmadm -id=sullivan -password=secret -consolemode -outfile=save.out</code>

Opciones de cliente de administración

En todas las modalidades del cliente de administración, se pueden utilizar las opciones para modificar las respuestas a la sesión del cliente de administración.

Sintaxis

```
          v                                     |
>>-DSMADM-----+-----+-----+----->
          '-opción_cliente_administración-'

>--+-----+-----+-----+-----<<
          '-mandato_servidor-'
```

Ejemplo de uso de opciones del cliente administrativo

Puede especificar el mandato DSMADM con su ID de usuario y su contraseña si utiliza las opciones -ID y -PASSWORD para que no se le solicite esa información. Para que IBM Spectrum Protect redirija toda la salida a un archivo, especifique la opción -OUTFILE con un nombre de archivo destino. Por ejemplo, para emitir el mandato QUERY NODE en modalidad de proceso por lotes con la salida redirigida al archivo SAVE.OUT, especifique:

```
dsmadm -id=sullivan -password=secret -outfile=save.out query node
```

Opciones

Las opciones de cliente de administración se pueden especificar con el mandato DSMADM y sólo son válidas desde una sesión de cliente de administración. Puede teclear una opción en letras mayúsculas, minúsculas o en cualquier combinación de mayúsculas/minúsculas. Las letras en mayúsculas indican la abreviatura más reducida que resulta aceptable. Si una opción aparece totalmente en letras mayúsculas, no se puede abreviar.

-ALWAYS Prompt

Especifica que se visualice un indicador de mandatos si la entrada se lleva a cabo desde el teclado o si es redirigida (por ejemplo, desde un archivo). Si no se especifica esta opción y se redirige la entrada, el indicador de mandatos no se graba.

Si la entrada se redirige, sólo se visualiza la salida del mandato. Si se especifica esta opción, se visualizan el indicador de mandatos y la salida de mandato.

-CHECKAliashalt

Permite al cliente de administración reconocer un alias para el mandato HALT tal como se ha establecido en la opción de servidor ALIASHALT. Consulte la publicación ALIASHALT para obtener más detalles.

-COMMA delimited

Especifica que cualquier salida tabular desde una consulta del servidor se ha de formatear como series separadas por comas, en lugar de en un formato legible. Esta opción está concebida para utilizarse principalmente al redirigir la salida de una consulta SQL (mandato SELECT). El formato de valores separados mediante comas es un formato de datos estándar que la mayoría de los programas comunes pueden procesar, incluidos las hojas de cálculo, las bases de datos y los programas de generación de informes.

-CONsolemode

Especifica que IBM Spectrum Protect se ejecuta en modalidad de consola. La mayor parte de la salida de consola del servidor se repite en la pantalla. La excepción son artículos tales como respuestas a mandatos de consulta que se emiten desde la consola, salida de rastreo o cualquier mensaje del sistema que se visualiza en la consola.

-DATAONLY=NO o YES

Especifica si la información de versión del producto y las cabeceras de salida se muestran con la salida. El valor predeterminado es NO.

NO

Especifica que se muestre la información de versión del producto y las cabeceras de columna de salida.

YES

Suprime la información de versión del producto y las cabeceras de columna de salida.

-DISPLaymode=LIST o TABLE

Puede forzar la salida QUERY en formato tabular o lista independientemente del ancho de columna de la ventana de línea de mandatos.

Si está utilizando la opción -DISPLAYMODE y desea que la salida vaya a un archivo, no especifique la opción -OUTFILE. Para escribir en el archivo utilice la redirección.

-ID=ID_usuario

Especifica el ID de usuario del administrador.

-Itemcommit

Especifica que IBM Spectrum Protect valida los mandatos que hay en un script o en una macro a medida que se procesa cada mandato.

-MOUNTmode

Especifica que IBM Spectrum Protect se ejecuta en modalidad de montaje. Todos los mensajes de montaje de medios extraíbles se repetirán su pantalla.

-NEWLINEAFTERPrompt

Especifica que un carácter de línea nueva debe escribirse después de que el indicador de mandatos y los mandatos que se han entrado desde el teclado se visualizan debajo de la petición. Si no se especifica esta opción, los mandatos especificados desde el teclado se visualizan en la parte derecha de la petición.

-NOConfirm

Especifica que no desea que IBM Spectrum Protect solicite confirmación antes de procesar mandatos que afectan a la disponibilidad del servidor o de los datos que gestiona el servidor.

-OUTfile

Especifica que la salida de una consulta del servidor se visualiza en una fila. Si la salida en una fila supera el ancho de columna que define el servidor, la salida se visualiza en varias líneas en dicha fila. Esta opción sólo está disponible en modalidad de proceso por lotes.

-OUTfile=nombreadarchivo

Especifica que la salida de un servidor se redirige a un archivo especificado. En la modalidad de proceso por lotes, la salida se redirige al archivo que especifique y el formato de la salida coincide con el formato de la salida de la pantalla.



En las sesiones de modalidad interactiva, de consola o de montaje, la salida se visualiza en la pantalla.



-PAssword=contraseña

Especifica la contraseña del administrador.

-Quiet

Especifica que IBM Spectrum Protect no visualiza mensajes de salida estándares en su pantalla. Sin embargo, cuando utilice esta opción, continuarán apareciendo determinados mensajes de error.

 Sistemas operativos AIX  Sistemas operativos Linux-SERveraddress

 Sistemas operativos AIX  Sistemas operativos Linux Especifica la stanza del servidor en el archivo dsm.sys. El cliente utiliza la stanza del servidor para determinar el servidor al que se conecta. La opción SERVERADDRESS está soportada por clientes administrativos que se ejecutan solo en sistemas operativos UNIX, Linux y Macintosh.

-TABdelimited

Especifica que cualquier salida tabular desde una consulta del servidor se ha de formatear como series separadas por tabulaciones en lugar de en un formato legible. Esta opción está concebida para utilizarse principalmente al redirigir la salida de una consulta SQL (mandato SELECT). El formato de valor separado por tabulaciones es un formato de datos estándar que pueden procesar muchos programas comunes, incluidos generadores de informes, de bases de datos y hojas de cálculo.

-TCPport

Especifica una dirección de puerto TCP/IP para un servidor de IBM Spectrum Protect. La opción TCPPORT solo está soportada por clientes de administración que se ejecutan en sistemas operativos Windows y es válida en la línea de mandatos del cliente de administración de Windows.

-TCPserveraddress


Especifica una dirección de servidor TCP/IP para un servidor de IBM Spectrum Protect. La opción TCPSEVERADDRESS sólo está soportada por clientes de administración que se ejecutan en sistemas operativos Windows y es válida en la línea de mandatos del cliente de administración de Windows.

Además de las opciones que se listan aquí, también puede especificar cualquier opción que se encuentra en el archivo de opciones del cliente. Cada opción debe tener antepuesto un guión y estar delimitada con un espacio.

Emisión de mandatos desde el Centro de operaciones

En la interfaz de mandatos del Centro de operaciones, puede emitir mandatos para gestionar servidores de IBM Spectrum Protect que están configurados como servidores concentradores o de radio.

Procedimiento

Para abrir la interfaz de línea de mandatos, pase el ratón sobre el icono de globo  en la barra de menús del Centro de operaciones y pulse Creador de mandatos.

Emisión de mandatos desde la consola del servidor

IBM Spectrum Protect proporciona un ID de usuario denominado SERVER_CONSOLE que permite emitir mandatos y administrar el servidor desde la consola del servidor después de instalar IBM Spectrum Protect. Durante la instalación, SERVER_CONSOLE se registra automáticamente como un administrador y se le otorga autorización del sistema.

Acerca de esta tarea

Si tiene privilegios del sistema, puede revocar u otorgar nuevos privilegios al ID de usuario SERVER_CONSOLE. No puede realizar ninguna de las acciones siguientes:

- Inscribir o actualizar el identificador de usuario SERVER_CONSOLE
- Bloquear o desbloquear el identificador de usuario SERVER_CONSOLE
- Redenominar el identificador de usuario SERVER_CONSOLE
- Suprimir el identificador de usuario SERVER_CONSOLE
- Direccional mandatos del identificador de usuario SERVER_CONSOLE

La consola del sistema no admite todos los mandatos de IBM Spectrum Protect. No se puede especificar el parámetro WAIT desde la consola del servidor.

Especificación de mandatos de administración

Los mandatos se componen de nombres de mandatos y suelen contener parámetros y variables. Los diagramas de sintaxis muestran las reglas que deben seguirse al especificar mandatos.

Acerca de esta tarea

Para mostrar la ayuda de línea de mandatos para los mandatos de servidor que tienen nombres exclusivos, puede escribir `help nombre_mandato`, donde *nombre_mandato* es el nombre del mandato de servidor para el que desea información. Por ejemplo, para mostrar ayuda para el mandato REGISTER NODE, escriba `help nodo de registro`. La sintaxis del mandato y las descripciones de parámetro se muestran en la salida.

Puede escribir también `help` seguido del número de tema del mandato. Los números de tema se muestran en la ayuda de línea de mandatos, por ejemplo:

```
3.0 Administrative commands
  3.46 REGISTER
    3.46.1 REGISTER ADMIN (Registrar un administrador)
    3.46.2 REGISTER LICENSE (Registrar una nueva licencia)
    3.46.3 REGISTER NODE (Registrar un nodo)
```

Para mostrar ayuda sobre el mandato REGISTER NODE, escriba:

```
help 3.46.3
```

Utilice números de tema para mostrar la ayuda de línea de mandatos para los submandatos. DEFINE DEVCLASS es un ejemplo de un mandato que tiene submandatos. Por ejemplo, puede especificar el mandato DEFINE DEVCLASS para las clases de dispositivo 3590 y para las clases de dispositivo 3592:

```
3.0 Administrative commands
  ...
  3.13.10 DEFINE DEVCLASS (Definir una clase de dispositivo)
    3.13.10.1 DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
    3.13.10.2 DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
    ...
```

Para mostrar ayuda para el mandato DEFINE DEVCLASS para las clases de dispositivo 3590, escriba:

```
help 3.13.10.1
```

- Lectura de los diagramas de sintaxis
Para leer un diagrama de sintaxis que indica cómo especificar un mandato, siga la ruta de la línea. Léalo de izquierda a derecha y de arriba a abajo.
- Utilización de caracteres de continuación para entrar mandatos largos
Los caracteres de continuación resultan útiles para procesar un mandato cuya longitud es mayor que la anchura de la pantalla o ventana. Puede utilizar caracteres de continuación en la modalidad interactiva del cliente de administración.
- Denominación de objetos de IBM Spectrum Protect
IBM Spectrum Protect restringe el número y tipo de caracteres que puede utilizar para nombrar objetos.
- Utilización de caracteres comodín para especificar nombres de objetos
En algunos mandatos, como por ejemplo los mandatos de consulta, puede utilizar caracteres comodín para crear una expresión que coincida con un patrón de modo que especifique más de un objeto. Utilizar caracteres comodín facilita la adaptación de un mandato a sus necesidades.
- Especificación de descripciones en parámetros de palabra clave
Si una descripción (una serie de texto) de un parámetro empieza por comillas simples o dobles o incluye blancos intercalado o signos igual, deberá especificar el valor entre comillas simples (') o dobles (").

Lectura de los diagramas de sintaxis

Para leer un diagrama de sintaxis que indica cómo especificar un mandato, siga la ruta de la línea. Léalo de izquierda a derecha y de arriba a abajo.

- El símbolo `>>---` indica el principio de un diagrama de sintaxis.
- El símbolo `---->` al final de una línea indica que el diagrama de sintaxis continúa en la línea siguiente.
- El símbolo `>---` al inicio de una línea indica que un diagrama de sintaxis es la continuación de la línea anterior.
- El símbolo `----><` indica el fin de un diagrama de sintaxis.

Nombres de mandato

El nombre del mandato puede componerse de una sola palabra de acción como, por ejemplo, HALT, o de una palabra de acción y de un objeto para la acción como, por ejemplo, DEFINE DOMAIN. Puede especificar el mandato en cualquier columna de la línea de entrada.

Especifique el nombre de mandato completo o la abreviatura especificada en el diagrama de sintaxis del mandato. Las letras en mayúsculas indican la abreviatura más reducida que resulta aceptable. Si un mandato aparece totalmente en letras mayúsculas, no se puede abreviar. Puede especificar el mandato en letras mayúsculas, letras minúsculas o en cualquier combinación de mayúsculas y minúsculas. En este ejemplo, puede entrar CMDNA, CMDNAM o CMDNAME en cualquier combinación de mayúsculas/minúsculas.

```
>>-CMDName-----><
```

Nota: Los nombres de mandato del texto descriptivo siempre se especifican en mayúsculas.

Parámetros necesarios

Cuando un parámetro está en la misma línea que el nombre del mandato, el parámetro es necesario. Cuando hay dos o más valores de parámetros en una pila y uno de ellos está en la línea, *debe* especificar un valor.

En este ejemplo, debe entrar PARMNAME=A, PARMNAME=B o PARMNAME=C. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>-PARMName-----A-----<<
      +-B-+
      '-C-'
```

Parámetros opcionales

Cuando un parámetro está debajo de la línea, dicho parámetro es opcional. En este ejemplo, puede especificar PARMNAME=A o no especificar nada. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>-+-----+-----<<
      '-PARMName-----A-'
```

Cuando dos o más valores de parámetro están en una pila debajo de la línea, todos son opcionales. En este ejemplo, puede especificar PARMNAME=A, PARMNAME=B, PARMNAME=C o no especificar nada. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>-+-----+-----<<
      '-PARMName-----A+-'
      +-B-+
      '-C-'
```

Valores predeterminados

Los valores predeterminados están sobre la línea. El sistema utiliza los valores predeterminados a menos que los modifique. Puede modificar temporalmente el valor predeterminado especificando una opción de la pila que se encuentra debajo de la línea.

En este ejemplo, PARMNAME=A es el valor predeterminado. También puede especificar PARMNAME=A, PARMNAME=B o PARMNAME=C. No incluya ningún espacio en blanco antes o después del signo igual (=).

```
.-PARMName-----A-----
>>-+-----+-----<<
      '-PARMName-----A+-'
      +-B-+
      '-C-'
```

Variables

Los elementos en minúsculas resaltados (de este modo) indican variables. En estos ejemplos, nombre_var representa las variables:

```
>>-CMDName--nombre_var-----<<
```

```
>>-+-----+-----<<
      '-PARMname-----nombre_var-'
```

Caracteres especiales

Debe codificar estos símbolos tal y como aparecen en el diagrama de sintaxis.

*
Asterisco
:


```

      Dos puntos
',
      Coma
=
      Signo de igual
-
      Guión
( )
      Paréntesis
.
      Punto

```

Repetición de valores

Una flecha de retorno hacia la izquierda significa que el elemento se puede repetir. Un carácter en la flecha significa que debe separar los elementos repetidos con dicho carácter.

```

      .-,-----
      V |
>>--nombre_archivo-+-----><

```

Elementos repetibles

Una pila de valores seguida de una flecha de retorno hacia la izquierda significa que puede seleccionar más de un valor o, si está permitido, repetir un mismo elemento. En este ejemplo, puede seleccionar más de un valor, delimitando cada nombre con una coma. No incluya ningún espacio en blanco antes o después del signo igual (=).

```

      .-,-----
      V |
>>-PARMName-----+valor1-+-+-----><
      +-valor2-+
      '-valor3-'

```

Notas a pie de página

Las notas a pie de página se incluyen entre paréntesis.

```

      .-,-----
      V (1) |
>>-----nombre_archivo-+-----><

```

Notas:

1. Puede especificar hasta cinco nombres de archivo.

Especificación de parámetros

El orden en que especifique los parámetros puede ser importante. En el siguiente ejemplo se muestra una parte del mandato que se utiliza para definir una agrupación de almacenamiento de copia:

```

>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
>--POOLtype----COpy--+-+----->
      '-DESCRiption----descripción-'
      .-REClaim----100-----
>-----><
      '-REClaim----porcentaje-'

```

Los primeros dos parámetros de este mandato (*nombre_agrupación* y *nombre_clase_dispositivo*) son parámetros necesarios. *nombre_agrupación* y *nombre_clase_dispositivo* también son posicionales. Es decir, deben especificarse en el orden que se muestra, inmediatamente después del nombre del mandato. El parámetro POOLTYPE es un parámetro de palabra clave necesario.

DESCRIPTION y RECLAIM son parámetros de palabra clave opcionales. Los parámetros de palabra clave se identifican con un signo igual que especifica un valor determinado o una variable. Los parámetros de palabra clave deben seguir a los parámetros posicionales en un mandato.

Todas las entradas de mandato siguientes, en las que los parámetros de palabra clave se ordenan de forma distinta, son aceptables:

```
define stgpool mycopypool mydeviceclass pooltype=copy
description=engineering
reclaim=50
define stgpool mycopypool mydeviceclass description=engineering
pooltype=copy
reclaim=50
```

El ejemplo siguiente, en el que uno de los parámetros de posición aparece a continuación de un parámetro de palabra clave, no es aceptable:

```
define stgpool mycopypool pooltype=copy mydeviceclass
description=engineering
reclaim=50
```

Fragmentos de sintaxis

Algunos diagramas, debido a su longitud, deben mostrar partes de la sintaxis en fragmentos. El nombre del fragmento aparece entre barras verticales en el diagrama.

El fragmento ampliado aparece en el diagrama después de una cabecera con el mismo nombre de fragmento. Una cabecera con el nombre de fragmento identifica el fragmento ampliado. Son necesarios mandatos que aparezcan directamente en la línea.

En este ejemplo, el fragmento se denomina "Fragmento".

```
>>| Fragmento |-----><
Fragmento
.-A-.
|-----|
+-B-+
'-C-'
```

Utilización de caracteres de continuación para entrar mandatos largos

Los caracteres de continuación resultan útiles para procesar un mandato cuya longitud es mayor que la anchura de la pantalla o ventana. Puede utilizar caracteres de continuación en la modalidad interactiva del cliente de administración.

Acerca de esta tarea

Sin caracteres de continuación, puede especificar hasta 256 caracteres. Con los caracteres de continuación, este límite se amplía a 1500 caracteres.

Nota: En el mandato MACRO, los valores máximos se aplican después de que se hayan aplicado variables de sustitución. Con los caracteres de continuación, puede efectuar lo siguiente:

- Especificar un guión al final de la línea que desea continuar.
Por ejemplo:

```
register admin pease mypasswd -
contact="david, ext1234"
```

- Continúe una lista de valores entrando un guión o una barra inclinada invertida, sin ningún espacio en blanco que le preceda, después de la última coma de la lista que entre en la primera línea. A continuación, entre los elementos restantes de la lista en la línea siguiente sin ningún espacio en blanco que le preceda. Por ejemplo:

```
stgpools=stg1,stg2,stg3,-
stg4,stg5,stg6
```

- Continúe una serie de valores que aparecen entre comillas entrando la primera parte de la serie que aparece entre comillas, seguida por un guión o barra inclinada invertida al final de la línea. A continuación, entre el resto de la serie en la línea siguiente, incluida en el mismo tipo de comillas.

Por ejemplo:

```
contact="david pease, bldg. 100, room 2b, san jose,"-  
"ext. 1234, alternate contact-norm pass,ext 2345"
```

IBM Spectrum Protect concatena las dos series sin espacios en blanco. Debe utilizar este método sólo para continuar una serie de valores entre comillas en más de una línea.

Denominación de objetos de IBM Spectrum Protect

IBM Spectrum Protect restringe el número y tipo de caracteres que puede utilizar para nombrar objetos.

Acerca de esta tarea

Puede utilizar los caracteres siguientes para definir nombres de objetos.

Carácter	Descripción
A-Z	Cualquier letra, A-Z
0-9	Cualquier número, 0-9
_	Subrayado
.	Punto
-	Guión
+	Más
&	Ampersand

La tabla siguiente muestra la longitud máxima de caracteres que se permite para asignar nombres a los objetos.

Tipo de nombre	Longitud máxima
Administradores, conjuntos de opciones de cliente, nodos cliente, contraseñas, grupos de servidores, nombres de servidores, nombres de espacios de archivos virtuales.	64
Identificadores de exportación reinicializable	64
Direcciones TCP/IP de alto y de bajo nivel (IPv4 o IPv6)	64
Clases de dispositivo, unidades, bibliotecas, clases de gestión, dominios de políticas, perfiles, scripts de planificación, juegos de copias de seguridad, agrupaciones de almacenamiento	30

Puede utilizar los caracteres siguientes para definir nombres de contraseñas:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Las contraseñas consideradas "LOCAL" son aquellas que se autentican con el servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas. Una vez actualizado un nodo o administrador para que utilice el parámetro SESSIONSECURITY=STRICT, la contraseña pasa a distinguir entre mayúsculas y minúsculas la siguiente vez que se cambia. Las contraseñas consideradas "LDAP" son aquellas que se autentican con un servidor de directorio LDAP y distinguen entre mayúsculas y minúsculas.

Cuando se utilizan mandatos DEFINE para definir volúmenes de base de datos, de anotaciones de recuperación y de agrupaciones de almacenamiento, el convenio de denominación del nombre del volumen depende del tipo de medio de acceso secuencial o medio de acceso aleatorio que esté utilizando. Consulte el VOLUME específico para obtener detalles.

Utilización de caracteres comodín para especificar nombres de objetos

En algunos mandatos, como por ejemplo los mandatos de consulta, puede utilizar caracteres comodín para crear una expresión que coincida con un patrón de modo que especifique más de un objeto. Utilizar caracteres comodín facilita la adaptación de un mandato a sus necesidades.

Acerca de esta tarea

Los caracteres comodín que utilice dependen del sistema operativo desde el que emite los mandatos. Por ejemplo, puede utilizar caracteres comodín, como un asterisco (*) en lugar de cualquier carácter (0 o más), o puede utilizar un signo de interrogación (?) o un signo de porcentaje (%) para hacer coincidir con exactitud un carácter.

La Tabla 1 proporciona referencias a los caracteres comodín para algunos sistemas operativos. Utilice los caracteres comodín adecuados a su sistema.

Tabla 1. Caracteres comodín por sistema operativo

Sistema operativo	Coincide cualquiera	Coincide exactamente uno
AIX, Linux, Windows	*	?
TSO	*	%

Por ejemplo, si desea consultar todas las clases de gestión cuyos nombres comiencen por DEV en todos los juegos de políticas de DOMAIN1, y su sistema utiliza un asterisco como el carácter para *cualquier coincidencia*, puede entrar:

```
query mgmtclass domain1 * dev*
```

Si su sistema utiliza el signo de interrogación como el carácter de *coincidencia exacta con un carácter* y desea consultar las clases de gestión en POLICYSET1 en DOMAIN1, puede escribir:

```
query mgmtclass domain1 policyset1 mc?
```

IBM Spectrum Protect visualizará la información sobre las clases de gestión que tengan los nombres MC.

La Tabla 2 muestra ejemplos adicionales sobre la utilización de caracteres comodín en lugar de cualquier carácter.

Tabla 2. Carácter de cualquier coincidencia

Patrón	Coincide con	No coincide con
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers

La Tabla 3 muestra ejemplos adicionales sobre el uso de caracteres comodín que coincidan exactamente con un carácter. El signo de interrogación (?) se puede sustituir por un signo de porcentaje (%) si la plataforma utiliza dicho carácter en lugar de (?).

Tabla 3. Carácter de coincidencia exacta

Patrón	Coincide con	No coincide con
ab?	abc	ab, abab, abzzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkrs

Especificación de descripciones en parámetros de palabra clave

Si una descripción (una serie de texto) de un parámetro empieza por comillas simples o dobles o incluye blancos intercalado o signos igual, deberá especificar el valor entre comillas simples (') o dobles (").

Acerca de esta tarea

Las comillas iniciales y finales tienen que ser del mismo tipo. Por ejemplo, si existe una comilla simple inicial, debe haber también una comilla simple final.

Por ejemplo, para registrar un nuevo nodo cliente denominado Louie, con una contraseña secret y con su cargo incluido como información de contacto, entre:

```
register node louie secret contact="manager of dept. 61f"
```

La tabla siguiente presenta los modos de especificar una descripción para el parámetro CONTACT. El valor puede contener comillas, espacios en blanco intercalados o signos de igual.

Para esta descripción	Especifique lo siguiente
manager	contact=manager
manager's	contact="manager's" o contact='manager's'
"manager"	contact=""manager"" o contact=""manager""
manager's report	contact="manager's report" o contact='manager's report'
manager's "report"	contact='manager's "report"'
manager=dept. 61f	contact='manager=dept. 61f'
manager reports to dept. 61f	contact='manager reports to dept. 61f' o contact="manager reports to dept. 61f"

Control del proceso de mandatos

Puede ejecutar algunos mandatos de IBM Spectrum Protect secuencialmente o simultáneamente con otros mandatos. También puede direccionar los mandatos de un servidor a otros servidores para su proceso.

Acerca de esta tarea

- Proceso de mandatos de servidor
IBM Spectrum Protect procesa los mandatos de administrador en primer plano o como proceso subordinado. Los mandatos que se procesan en primer plano deben haber finalizado para poder emitir otro mandato. Cuando los mandatos se procesan en un proceso subordinado, puede emitir mandatos adicionales en cualquier momento.
- Detener procesos en segundo plano
Utilice el mandato CANCEL PROCESS para cancelar los mandatos que generan procesos subordinados.

Proceso de mandatos de servidor

IBM Spectrum Protect procesa los mandatos de administrador en primer plano o como proceso subordinado. Los mandatos que se procesan en primer plano deben haber finalizado para poder emitir otro mandato. Cuando los mandatos se procesan en un proceso subordinado, puede emitir mandatos adicionales en cualquier momento.

La mayor parte de los mandatos de IBM Spectrum Protect se procesan en primer plano. En el caso de algunos mandatos que normalmente se procesan en un proceso subordinado (por ejemplo, BACKUP DB), puede especificar el parámetro WAIT (WAIT=YES) para que el mandato se procese en primer plano. Es posible que desee procesar un mandato en primer plano en lugar de hacerlo en segundo plano por alguno de estos motivos:

- Para determinar rápidamente si un mandato se ha completado correctamente. Cuando se emite un mandato que se procesa en primer plano, IBM Spectrum Protect envía un mensaje de confirmación que indica que el mandato ha finalizado correctamente. Si procesa el mandato en segundo plano, necesitará abrir informes de operaciones o consultar el registro de actividad para determinar si el mandato ha finalizado correctamente.
- Para supervisar las actividades del servidor (por ejemplo, los mensajes) en el cliente administrativo mientras se está procesando un mandato. Esto puede ser preferible a realizar búsquedas en un registro de actividades largo después de que el mandato haya finalizado.
- Para poder iniciar otro proceso de inmediato después de que haya finalizado un mandato. Por ejemplo, podría especificar WAIT=YES para un mandato que no tarde mucho en procesarse, de manera que cuando finalice pueda iniciar el proceso de otro mandato de inmediato.
- Para serializar los mandatos de un script administrativo cuando sea importante que un mandato finalice antes de que otro empiece.

Compruebe la descripción del mandato individual para determinar si el mandato tiene un parámetro WAIT.

Puede cancelar los mandatos que se procesan en primer plano desde la consola del servidor o desde otra sesión de cliente de administración.

A cada proceso subordinado se le asigna un número de proceso. Utilice el mandato QUERY PROCESS para obtener el estado y el número de proceso de un proceso subordinado.

Nota:

- Si va a definir una planificación con un mandato que especifica WAIT=NO (valor predeterminado) y emite QUERY EVENT para determinar el estado de la operación planificada, las operaciones con errores notificarán un estado de evento COMPLETED con

un código de retorno OK. Para que la salida de QUERY EVENT eflaje el estado de error, el parámetro WAIT debe establecerse en YES. Esto ejecuta la operación planificada en primer plano y le informa del estado cuando finalice.

- No puede procesar mandatos en primer plano desde la consola del servidor.

Detener procesos en segundo plano

Utilice el mandato CANCEL PROCESS para cancelar los mandatos que generan procesos subordinados.

Acerca de esta tarea

Utilice el mandato QUERY PROCESS para obtener el estado y el número de proceso de un proceso subordinado. Si un proceso subordinado está activo cuando lo cancela, el servidor detiene el proceso. Cualquier cambio que no se haya validado se suprimirá por caducidad. Sin embargo, los cambios validados no se suprimirán por caducidad.

Cuando emite un mandato QUERY desde el cliente de administración, se podrían generar varias pantallas de salida. Si esto ocurre no es necesaria una salida adicional, el administrador puede cancelar la pantalla de salida a la estación de trabajo cliente. Si lo hace, no finalizará el proceso del mandato.

Realización de tareas simultáneamente en varios servidores

El direccionamiento de mandatos permite direccionar los mandatos a uno o más servidores para que los procesen y, a continuación, recopilar la salida de estos servidores.

Acerca de esta tarea

Para direccionar mandatos a otros servidores, es necesario que tenga el mismo ID y contraseña de administrador así como la autorización de administración exigida en todos los servidores a los que se redirecciona el mandato. No puede direccionar mandatos a otros servidores desde la consola del servidor.

Una vez se ha terminado de procesar el mandato en todos los servidores, se visualiza la salida completa para cada servidor. Por ejemplo, la salida de SERVER_A se visualiza totalmente, seguida de la salida de SERVER_B. La salida incluye mensajes de resumen para cada servidor e identifica el servidor que ha procesado la salida. Los códigos de retorno indican si los mandatos se han procesado correctamente en los servidores. Estos códigos de retorno incluyen una de tres gravedades: 0, ERROR o WARNING.

Todo servidor que se identifica como el destino de un mandato direccionado debe definirse primero mediante el mandato DEFINE SERVER. El mandato se direcciona automáticamente a todos los servidores especificados como miembros de un grupo de servidores o a los servidores individuales especificados con el mandato.

Los ejemplos siguientes describen cómo direccionar el mandato QUERY STGPOOL a un servidor, a varios servidores, a un grupo de servidores, a varios grupos de servidores, o a una combinación de servidores y grupos de servidores. Cada servidor o grupo de servidores de una lista debe estar separado con una coma, sin espacios.

Direccionamiento de mandatos a un único servidor

Procedimiento

Para direccionar el mandato QUERY STGPOOL al servidor denominado ASTRO, entre:

```
astro: query stgpool
```

Con dos puntos después del nombre de servidor se indica el fin de la información de direccionamiento. Esto se denomina el *prefijo del servidor*. Otra forma de indicar que la información de direccionamiento ha terminado es encerrar entre paréntesis el nombre del servidor, por ejemplo:

```
(astro) query stgpool
```

Direccionamiento de mandatos a varios servidores

Acerca de esta tarea

Procedimiento

Para direccionar el mandato QUERY STGPOOL a varios servidores denominados HD_QTR, MIDAS, SATURN, entre:

```
hd_qtr,midas,saturn: query stgpool
```

Si el primer servidor no está definido en IBM Spectrum Protect, el mandato se direccionará al siguiente servidor definido de la lista de servidores.

También puede especificar el mandato de este modo:

```
(hd_qtr,midas,saturn) query stgpool
```

Direccionamiento de mandatos a un grupo de servidores

Acerca de esta tarea

En este ejemplo, el grupo de servidores ADMIN tiene los servidores denominados SECURITY, PAYROLL y PERSONNEL definidos como miembros del grupo. El mandato se direccionará a cada uno de estos servidores.

Procedimiento

Para direccionar el mandato QUERY STGPOOL al grupo de servidores llamado ADMIN, especifique:

```
admin: query stgpool
```

También puede especificar el mandato de este modo:

```
(admin) query stgpool
```

Direccionamiento de mandatos a grupos de servidores

Acerca de esta tarea

En este ejemplo, el grupo de servidores ADMIN2 tiene los servidores SERVER_A, SERVER_B y SERVER_C definidos como miembros del grupo, y el grupo de servidores ADMIN3 tiene los servidores ASTRO, GUMBY y CRUSTY definidos como miembros del grupo. El mandato se direccionará a los servidores SERVER_A, SERVER_B, SERVER_C, ASTRO, GUMBY y CRUSTY.

Procedimiento

Para direccionar el mandato QUERY STGPOOL a dos grupos de servidores denominados ADMIN2 y ADMIN3, especifique:

```
admin2,admin3: query stgpool
```

También puede especificar el mandato de este modo:

```
(admin2,admin3) query stgpool
```

Direccionamiento de mandatos a dos servidores y un grupo de servidores

Acerca de esta tarea

En este ejemplo, el grupo de servidores DEV_GROUP tiene los servidores SALES, MARKETING y STAFF definidos como miembros del grupo. El mandato se direccionará a los servidores SALES, MARKETING, STAFF, MERCURY y JUPITER.

Procedimiento

Para direccionar el mandato QUERY STGPOOL al grupo de servidores denominado DEV_GROUP y a los servidores denominados MERCURY y JUPITER, entre:

```
dev_group,mercury,jupiter: query stgpool
```

También puede especificar el mandato de este modo:

```
(dev_group,mercury,jupiter) query stgpool
```

Direccionamiento de mandatos dentro de scripts

Acerca de esta tarea

Si direcciona mandatos dentro de los scripts, debe delimitar el servidor o el grupo de servidores con paréntesis y omitir los dos puntos. De lo contrario, el mandato no se direccionará al emitir el mandato RUN y sólo se ejecutará en el servidor donde se emite el mandato RUN.

Por ejemplo, para direccionar el mandato QUERY STGPOOL dentro de un script:

Procedimiento

1. Se definirá el script denominado QU_STG para direccionarlo al grupo de servidores DEV_GROUP.

```
define script qu_stg "(dev_group) query stgpool"
```

2. Se ejecutará el script QU_STG:

```
run qu_stg
```

Resultados

En este ejemplo, el grupo de servidores DEV_GROUP tiene los servidores SALES, MARKETING y STAFF definidos como miembros del grupo. El mandato QUERY STGPOOL se direccionará a estos servidores.

Clases de privilegio

La autorización que se otorga a un administrador mediante la clase de privilegio determina qué mandatos de administración puede emitir el administrador.

Existen cuatro clases de privilegios de administrador en IBM Spectrum Protect:

- Sistema
- Política
- Almacenamiento
- Operador

Después de que un administrador se ha registrado mediante la utilización del mandato REGISTER ADMIN, el administrador puede emitir un conjunto limitado de mandatos, incluidos todos los mandatos de consulta. Cuando se instala IBM Spectrum Protect, la consola del servidor se define como un administrador del sistema denominado SERVER_CONSOLE y se le otorga privilegio de sistema.

- Mandatos que requieren privilegio de sistema
Un administrador con privilegio de sistema tiene el nivel de autorización más alto para el servidor. Con el privilegio de sistema un administrador puede emitir cualquier mandato de administración y posee autorización para gestionar todos los dominios de políticas y todas las agrupaciones de almacenamiento.
- Mandatos que requieren privilegio de políticas
Un administrador con privilegio de políticas puede emitir mandatos relacionados con objetos de gestión de políticas, como dominios de políticas, juegos de políticas, clases de gestión, grupos de copia y planificaciones. El privilegio de políticas puede no tener restricciones o puede estar restringido a agrupaciones de dominios de política específicos.
- Mandatos que requieren privilegio de almacenamiento
Un administrador con privilegio de almacenamiento puede emitir mandatos que asignen y controlen recursos de almacenamiento para el servidor. El privilegio de almacenamiento puede no tener restricciones o puede estar restringido a agrupaciones de almacenamiento específicas.
- Mandatos que requieren privilegio de operador
Un administrador con privilegio de operador puede emitir mandatos que controlan la operación inmediata del servidor y la disponibilidad del medio de almacenamiento.
- Mandatos que puede emitir cualquier administrador
Existen algunos mandatos que pueden ser utilizados por cualquier administrador, incluso si no se le ha otorgado ningún privilegio de administrador específico.

Mandatos que requieren privilegio de sistema

Un administrador con privilegio de sistema tiene el nivel de autorización más alto para el servidor. Con el privilegio de sistema un administrador puede emitir cualquier mandato de administración y posee autorización para gestionar todos los dominios de políticas y todas las agrupaciones de almacenamiento.

La Tabla 1 lista los mandatos que pueden emitir los administradores que posean privilegio de sistema. En algunos casos, los administradores con niveles inferiores de autorización, como por ejemplo el privilegio de almacenamiento sin restricciones, también pueden emitir estos mandatos. Además, la opción de servidor REQSYSAUTHOUTFILE puede utilizarse para especificar que determinados mandatos requieren privilegios del sistema si provocan que el servidor grabe en un archivo externo. Para obtener más información sobre esta opción de servidor, revise REQSYSAUTHOUTFILE.

Tabla 1. Mandatos de privilegio de sistema

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> • AUDIT LDAPDIRECTORY • AUDIT LICENSES • ACCEPT DATE • BEGIN EVENTLOGGING • CANCEL EXPIRATION • CANCEL PROCESS • CANCEL REPLICATION • CANCEL REQUEST • CANCEL RESTORE • CLEAN DRIVE • COPY ACTIVATEDATA • COPY DOMAIN • COPY POLICYSET • COPY PROFILE • COPY SCHEDULE (Nota de revisión.) • COPY SCRIPT • COPY SERVERGROUP • DEFINE BACKUPSET • DEFINE CLIENTACTION • DEFINE CLIENTOPT • DEFINE CLOPTSET • DEFINE COLLOGGROUP • DEFINE COLLOCMEMBER • DEFINE DEVCLASS • DEFINE DOMAIN • DEFINE DRIVE • DEFINE EVENTSERVER • DEFINE GRPMEMBER • DEFINE LIBRARY • DEFINE MACHINE • DEFINE MACHNODEASSOCIATION • DEFINE NODEGROUP • DEFINE NODEGROUPMEMBER • DEFINE PATH • DEFINE PROFASSOCIATION • DEFINE PROFILE • DEFINE RECMEDMACHASSOCIATION • DEFINE RECOVERYMEDIA • DEFINE SCHEDULE (Nota de revisión.) • DEFINE SCRIPT • DEFINE SERVER • DEFINE SERVERGROUP 	<ul style="list-style-type: none"> • DEFINE SPACETRIGGER • DEFINE STGPOOL • DEFINE SUBSCRIPTION • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME • DELETE BACKUPSET • DELETE CLIENTOPT • DELETE CLOPTSET • DEFINE COLLOGGROUP • DEFINE COLLOCMEMBER • DELETE DOMAIN • DELETE DRIVE • DELETE EVENTSERVER • DELETE GRPMEMBER • DELETE LIBRARY • DELETE MACHINE • DELETE MACHNODEASSOCIATION • DELETE NODEGROUP • DELETE NODEGROUPMEMBER • DELETE PROFASSOCIATION • DELETE PROFILE • DELETE RECMEDMACHASSOCIATION • DELETE RECOVERYMEDIA • DELETE SCHEDULE (Nota de revisión.) • DELETE SCRIPT • DELETE SERVER • DELETE SERVERGROUP • DELETE SPACETRIGGER • DELETE STGPOOL • DELETE SUBSCRIBER • DELETE SUBSCRIPTION • DELETE VIRTUALFSMAPPING • DISABLE EVENTS • ENABLE EVENTS • END EVENTLOGGING • EXPIRE INVENTORY • EXPORT ADMIN • EXPORT NODE • EXPORT POLICY • EXPORT SERVER • GENERATE BACKUPSET • GRANT AUTHORITY

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> • GRANT PROXYNODE • IDENTIFY DUPLICATES • IMPORT NODE • IMPORT POLICY • IMPORT SERVER • INSERT MACHINE • LABEL LIBVOLUME • LOCK ADMIN • LOCK PROFILE • MIGRATE STGPOOL • MOVE DRMEDIA • MOVE MEDIA • MOVE GRPMEMBER • NOTIFY SUBSCRIBERS • PERFORM LIBACTION • PING SERVER • PREPARE • QUERY BACKUPSETCONTENTS • QUERY MEDIA • QUERY RPFCONTENT • QUERY TOC • RECLAIM STGPOOL • RECONCILE VOLUMES • REGISTER ADMIN • REGISTER LICENSE • REMOVE ADMIN • REMOVE REPLNODE • RENAME ADMIN • RENAME SCRIPT • RENAME SERVERGROUP • RENAME STGPOOL • REPLICATE NODE • RESET PASSEXP • RESTORE NODE • REVOKE AUTHORITY • REVOKE PROXYNODE • RUN • SET ACCOUNTING • SET ACTLOGRETENTION • SET ARCHIVERETENTIONPROTECTION • SET ARREPLRULEDEFAULT • SET BKREPLRULEDEFAULT • SET CLIENTACTDURATION 	<ul style="list-style-type: none"> • SET CONFIGMANAGER • SET CONFIGREFRESH • SET CONTEXTMESSAGING • SET CROSSDEFINE • SET DBRECOVERY • SET DEFAULTAUTHENTICATION • SET DRMACTIVEDATASTGPOOL • SET DRMCHECKLABEL • SET DRMCMDFILENAME • SET DRMCOPYCONTAINERSTGPOOL • SET DRMCOPYSTGPOOL • SET DRMCOURIERNAME • SET DRMDBBACKUPEXPIREDAYS • SET DRMFILEPROCESS • SET DRMINSTRPREFIX • SET DRMNOTMOUNTABLENAME • SET DRMPPLANPREFIX • SET DRMPPLANVPOSTFIX • SET DRMPRIMSTGPOOL • SET DRMRPFEXPIREDAYS • SET DRMVaultNAME • SET EVENTRETENTION • SET INVALIDPWLIMIT • SET LDAPPASSWORD • SET LDAPUSER • SET LICENSEAUDITPERIOD • SET MAXCMDRETRIES • SET MAXSCHEDESSESSIONS • SET MINPWLENGTH • SET PASSEXP • SET QUERYSCHEDPERIOD • SET RANDOMIZE • SET REPLRETENTION • SET REPLSERVER • SET RETRYPERIOD • SET SCHEDMODES • SET SERVERHLADDRESS • SET SERVERLLADDRESS • SET SERVERNAME • SET SERVERPASSWORD • SET SPREPLRULEDEFAULT • SET SUBFILE • SET TOCLOADRETENTION
<ul style="list-style-type: none"> • SETOPT • UNLOCK ADMIN • UNLOCK PROFILE • UPDATE ADMIN • UPDATE BACKUPSET • UPDATE CLIENTOPT • UPDATE CLOPTSET • UPDATE COLLOGROUP • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE LIBVOLUME • UPDATE MACHINE 	<ul style="list-style-type: none"> • UPDATE NODEGROUP • UPDATE PATH • UPDATE PROFILE • UPDATE RECOVERYMEDIA • UPDATE REPLRULE • UPDATE SCHEDULE (Nota de revisión.) • UPDATE SCRIPT • UPDATE SERVER • UPDATE SERVERGROUP • UPDATE SPACETRIGGER • UPDATE VIRTUALFSMAPPING • UPDATE VOLHISTORY • VALIDATE LANFREE • VALIDATE REPLICATION
<p>Nota: Este mandato está limitado por la autoridad que se otorga como administrador. El privilegio de sistema sólo es necesario para las planificaciones de mandatos de administración. El privilegio de sistema o de políticas es necesario para las planificaciones de operaciones de cliente.</p>	

Mandatos que requieren privilegio de políticas

Un administrador con privilegio de políticas puede emitir mandatos relacionados con objetos de gestión de políticas, como dominios de políticas, juegos de políticas, clases de gestión, grupos de copia y planificaciones. El privilegio de políticas puede no tener restricciones o puede estar restringido a agrupaciones de dominios de política específicos.

El privilegio de políticas sin restricciones le permite emitir todos los mandatos de administrador que requieran privilegio de políticas. Puede emitir mandatos que afecten a todos los dominios de políticas existentes, al igual que a cualquier dominio de políticas que se defina más adelante. Un administrador con privilegio de políticas sin restricciones no puede definir, suprimir o copiar dominios de políticas.

El privilegio de políticas con restricciones le permite emitir mandatos de administrador que afectan a uno o más dominios de políticas para los que se le ha otorgado autorización. Por ejemplo, el mandato DELETE MGMTCLASS requiere que tenga privilegio de políticas para el dominio de políticas al que pertenece la clase de gestión.

La Tabla 1 lista los mandatos que puede emitir un administrador con privilegio de políticas.

Tabla 1. Mandatos de privilegio de políticas

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none">• ACTIVATE POLICYSET• ASSIGN DEFMGMTCLASS• CLEAN DRIVE• BACKUP NODE• COPY MGMTCLASS• COPY POLICYSET• COPY SCHEDULE (Revise nota 2.)• DEFINE ASSOCIATION• DEFINE BACKUPSET• DEFINE COPYGROUP• DEFINE CLIENTACTION• DEFINE CLIENTOPT• DEFINE MGMTCLASS• DEFINE NODEGROUP• DEFINE NODEGROUPMEMBER• DEFINE POLICYSET• DEFINE SCHEDULE• DELETE ASSOCIATION• DELETE BACKUPSET• DELETE COPYGROUP• DELETE EVENT (Revise nota 1.)• DELETE FILESPACE• DELETE MGMTCLASS• DELETE NODEGROUP• DELETE NODEGROUPMEMBER	<ul style="list-style-type: none">• DELETE POLICYSET• DELETE PATH• DELETE SCHEDULE (Revise nota 2.)• GENERATE BACKUPSET• LOCK NODE• QUERY BACKUPSETCONTENTS• REGISTER NODE• REMOVE NODE• RENAME FILESPACE• RENAME NODE• SET SUMMARYRETENTION• RESTORE NODE• QUERY TOC• UNLOCK NODE• UPDATE BACKUPSET• UPDATE COPYGROUP• UPDATE DOMAIN• UPDATE MGMTCLASS• UPDATE NODE• UPDATE NODEGROUP• UPDATE POLICYSET• UPDATE SCHEDULE (Revise nota 2.)• VALIDATE POLICYSET
<p>Notas:</p> <ol style="list-style-type: none">1. Este mandato puede estar limitado a un dominio de políticas. Un administrador con privilegio de políticas sin restricciones o privilegio de políticas limitado a un dominio de políticas especificado puede emitir este mandato.2. Este mandato está limitado por la autoridad que se otorga como administrador. El privilegio de sistema sólo es necesario para las planificaciones de mandatos de administración. El privilegio de sistema o de políticas es necesario para las planificaciones de operaciones de cliente.	

Mandatos que requieren privilegio de almacenamiento

Un administrador con privilegio de almacenamiento puede emitir mandatos que asignen y controlen recursos de almacenamiento para el servidor. El privilegio de almacenamiento puede no tener restricciones o puede estar restringido a agrupaciones de almacenamiento específicas.

El privilegio de almacenamiento sin restricciones le permite emitir todos los mandatos de administrador que requieran privilegio de almacenamiento. Puede emitir mandatos que afecten a todas las agrupaciones de almacenamiento existentes, al igual que a cualquier agrupación de almacenamiento que se defina más adelante. También puede emitir mandatos que afecten a la base de datos y a las

anotaciones de recuperación. Un administrador con privilegio de almacenamiento sin restricciones no puede definir ni suprimir agrupaciones de almacenamiento.

El privilegio de almacenamiento con restricciones le permite emitir mandatos de administrador que afectan únicamente a una agrupación de almacenamiento para la que se le ha otorgado autorización. Por ejemplo, el mandato DELETE VOLUME únicamente afecta a un volumen de agrupación de almacenamiento que se ha definido en una agrupación de almacenamiento específica.

La Tabla 1 lista los mandatos que puede emitir un administrador con privilegio de almacenamiento.

Tabla 1. Mandatos de privilegio de almacenamiento

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> • AUDIT LIBRARY • AUDIT VOLUME (Nota de revisión.) • BACKUP DB • BACKUP DEVCONFIG • BACKUP STGPOOL • BACKUP VOLHISTORY • CHECKIN LIBVOLUME • CHECKOUT LIBVOLUME • COPY ACTIVATEDATA (Nota de revisión.) • DEFINE COLLOGGROUP • DEFINE COLLOCMEMBER • DEFINE DATAMOVER • DEFINE DEVCLASS • DEFINE DRIVE • DEFINE LIBRARY • DEFINE PATH • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME (Nota de revisión.) • DEFINE SPACETRIGGER • DELETE COLLOGGROUP • DELETE COLLOCMEMBER • DELETE DATAMOVER • DELETE DEVCLASS • DELETE DRIVE • DELETE LIBRARY • DELETE PATH 	<ul style="list-style-type: none"> • DELETE SPACETRIGGER • DELETE VIRTUALFSMAPPING • DELETE VOLHISTORY • DELETE VOLUME (Nota de revisión.) • GRANT PROXYNODE • LABEL LIBVOLUME • MIGRATE STGPOOL • MOVE DATA (Nota de revisión.) • MOVE MEDIA • QUERY TAPEALERTMSG • RECLAIM STGPOOL • RESTORE STGPOOL • RESTORE VOLUME • REVOKE PROXYNODE • SET TAPEALERTMSG • UPDATE COLLOGGROUP • UPDATE DATAMOVER • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE PATH • UPDATE SPACETRIGGER • UPDATE STGPOOL (Nota de revisión.) • UPDATE VIRTUALFSMAPPING
<p>Nota: Este mandato puede estar limitado a una agrupación de almacenamiento. Un administrador con privilegio de almacenamiento sin restricciones o privilegio de almacenamiento limitado a una agrupación de almacenamiento especificada puede emitir este mandato.</p>	

Mandatos que requieren privilegio de operador

Un administrador con privilegio de operador puede emitir mandatos que controlan la operación inmediata del servidor y la disponibilidad del medio de almacenamiento.

La Tabla 1 lista los mandatos que un administrador con privilegio de operador puede emitir.

Tabla 1. Mandatos de privilegio de operador

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> • CANCEL SESSION • DISABLE SESSIONS • DISMOUNT VOLUME • ENABLE SESSIONS • HALT 	<ul style="list-style-type: none"> • MOVE DRMEDIA • MOVE MEDIA • QUERY MEDIA • REPLY • UPDATE VOLUME • VARY

Mandatos que puede emitir cualquier administrador

Existen algunos mandatos que pueden ser utilizados por cualquier administrador, incluso si no se le ha otorgado ningún privilegio de administrador específico.

La Tabla 1 lista los mandatos que cualquier administrador registrado puede emitir.

Tabla 1. Mandatos emitidos por todos los administradores

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> • COMMIT • HELP • ISSUE MESSAGE • MACRO • PARALLEL • QUERY ACTLOG • QUERY ADMIN • QUERY ASSOCIATION • QUERY AUDITOCUPANCY • QUERY BACKUPSET • QUERY CLOPSET • QUERY COLLOGGROUP • QUERY CONTENT • QUERY COPYGROUP • QUERY DATAMOVER • QUERY DB • QUERY DBSPACE • QUERY DEVCLASS • QUERY DIRSPACE • QUERY DOMAIN • QUERY DRIVE • QUERY DRMEDIA • QUERY DRMSTATUS • QUERY ENABLED • QUERY EVENT • QUERY EVENTRULES • QUERY EVENTSERVER • QUERY FILESPACE • QUERY LIBRARY • QUERY LIBVOLUME • QUERY LICENSE • QUERY LOG • QUERY MACHINE • QUERY MGMTCLASS • QUERY MOUNT • QUERY NASBACKUP 	<ul style="list-style-type: none"> • QUERY NODE • QUERY NODEDATA • QUERY NODEGROUP • QUERY OCCUPANCY • QUERY OPTION • QUERY PATH • QUERY POLICYSET • QUERY PROCESS • QUERY PROFILE • QUERY PROXYNODE • QUERY RECOVERYMEDIA • QUERY REPLICATION • QUERY REPLNODE • QUERY REPLRULE • QUERY REQUEST • QUERY RESTORE • QUERY RPFIL • QUERY SCHEDULE • QUERY SCRIPT • QUERY SERVER • QUERY SERVERGROUP • QUERY SESSION • QUERY SPACETRIGGER • QUERY STATUS • QUERY STGPOOL • QUERY SUBSCRIBER • QUERY SUBSCRIPTION • QUERY SYSTEM • QUERY • VIRTUALFSMAPPING • QUERY VOLHISTORY • QUERY VOLUME • QUIT • ROLLBACK • SELECT • SERIAL

Mandatos de administración

Los mandatos de administración están disponibles para gestionar y configurar el servidor.

La información sobre cada mandato incluye:

- Una descripción de las tareas que realiza un mandato
 - La clase de privilegio del administrador que es necesaria para utilizar el mandato
 - Un diagrama de sintaxis que identifica los parámetros necesarios y opcionales del mandato
 - Las descripciones de cada uno de los parámetros del mandato
 - Ejemplos de cómo utilizar el mandato
 - Una lista de los mandatos relacionados
- ACCEPT DATE (aceptar la fecha del sistema actual)
Utilice este mandato para que el servidor pueda iniciar un proceso normal, cuando el servidor no inicia un proceso normal a causa de una discrepancia entre la fecha del servidor y la fecha actual del sistema.
 - ACTIVATE POLICYSET (Activar un nuevo juego de políticas)
Utilice este mandato para copiar el contenido de un juego de políticas en el juego de políticas ACTIVE del dominio. El servidor utiliza las reglas del juego de políticas ACTIVE para gestionar las operaciones de cliente en el dominio. Puede definir varios

juegos de políticas para un dominio de políticas, pero únicamente puede haber un juego de políticas activo. El juego de políticas ACTIVE actual se sustituye por el que especifique al emitir este mandato. Sólo puede modificar el juego de políticas ACTIVE activando otro juego de políticas.

- **ASSIGN DEFMGMTCLASS** (asignar una clase de gestión predeterminada)
Utilice este mandato para especificar una clase de gestión como la clase de gestión predeterminada para un juego de políticas. Para poder activar el juego de políticas, debe asignar una clase de gestión predeterminada a un juego de políticas.
- **Mandatos AUDIT**
Utilice los mandatos AUDIT para revisar o examinar si tanto la información de la base de datos como el volumen de agrupación de almacenamiento están en un estado correcto. El mandato AUDIT LDAPDIRECTORY elimina los nodos o ID de administrador de un servidor de directorio LDAP, que no autentican sus contraseñas con el servidor de directorio LDAP.
- **Mandatos BACKUP**
Utilice los mandatos BACKUP para crear copias de seguridad de información u objetos IBM Spectrum Protect.
- **BEGIN EVENTLOGGING** (Iniciar anotación de eventos)
Utilice este mandato para empezar a anotar eventos en uno o varios receptores. Un receptor para el que se ha iniciado la anotación de eventos es un *receptor activo*.
- **Mandatos CANCEL**
Utilice el mandato CANCEL para finalizar una tarea o un proceso antes de que se haya completado.
- **CHECKIN LIBVOLUME** (Dar de alta un volumen de almacenamiento en una biblioteca)
Utilice este mandato para agregar un volumen de acceso secuencial o una cinta de limpieza al inventario del servidor para una biblioteca automatizada. El servidor utilizará un volumen que resida físicamente en una biblioteca automatizada hasta que dicho volumen se haya dado de alta.
- **CHECKOUT LIBVOLUME** (Dar de baja un volumen de almacenamiento de una biblioteca)
Utilice este mandato para suprimir del inventario del servidor un volumen de almacenamiento de acceso secuencial de una biblioteca automatizada. Este mandato crea un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.
- **CLEAN DRIVE** (Limpiar una unidad)
Utilice este mandato si desea que IBM Spectrum Protect cargue inmediatamente un cartucho limpiador en una unidad al margen de la frecuencia de limpieza.
- **COMMIT** (controlar la validación de mandatos en una macro)
Utilice este mandato para controlar cuándo se valida un mandato en una macro y para actualizar la base de datos cuando los mandatos terminan el proceso. Si se emite en la modalidad de consola del cliente de administración, este mandato no genera ningún mensaje.
- **CONVERT STGPOOL** (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)
Utilice este mandato para convertir una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Puede utilizar agrupaciones de almacenamiento de contenedores para la deduplicación de datos del lado de cliente y en línea.
- **Mandatos COPY**
Utilice los mandatos COPY para crear una copia de los objetos o datos de IBM Spectrum Protect.
- **DEACTIVATE DATA** (Desactivar datos para un nodo de cliente)
Utilice este mandato para especificar que los datos activos que se han copiado para un nodo de cliente de aplicaciones antes de una fecha especificada ya no son necesarios. El mandato marca los datos como inactivos para que puedan suprimirse de acuerdo con las políticas de retención de datos.
- **Mandatos DECOMMISSION**
Utilice los mandatos DECOMMISSION para eliminar nodos cliente del entorno de producción. Los nodos de cliente pueden ser aplicaciones, sistemas y máquinas virtuales.
- **Mandatos DEFINE**
Utilice los mandatos DEFINE para crear objetos de IBM Spectrum Protect.
- **Mandatos DELETE**
Utilice los mandatos DELETE para suprimir o eliminar un objeto de IBM Spectrum Protect.
- **Mandatos DISABLE**
Utilice los mandatos DISABLE para que el servidor no pueda realizar determinados tipos de operaciones.
- **Mandatos DISMOUNT**
Utilice el mandato DISMOUNT para desmontar un volumen mediante la dirección de dispositivo real o mediante el nombre de volumen.
- **DISPLAY OBJNAME** (Mostrar un nombre de objeto completo)
Utilice este mandato para IBM Spectrum Protect que se visualice un nombre de objeto completo si el nombre que figura en un mensaje o en la salida de una consulta está abreviado por razones de limitación de longitud. Los nombres de objeto que son muy largos pueden ser difíciles de mostrar y usar en funciones normales del sistema operativo. El servidor IBM Spectrum Protect abreviará nombres largos y les asignará un ID de señal que puede utilizarse si el nombre de la ruta del objeto sobrepasa los 1024 bytes. El ID de señal se muestra en una cadena que incluye identificadores para el nodo, el espacio de archivos y el nombre del objeto. El formato es: [TSMOBJ:*nID.fsID.objID*]. Cuando se especifica con el mandato DISPLAY OBJNAME, el ID de señal puede utilizarse para que se muestre el nombre completo del objeto.

- Mandatos ENABLE
Utilice el mandato ENABLE para que el servidor pueda realizar algunos tipos de operaciones.
- ENCRYPT STGPOOL (Cifrar datos en una agrupación de almacenamiento)
Utilice este mandato para cifrar datos en una agrupación de almacenamiento de contenedores de directorio o de contenedores de nube.
- END EVENTLOGGING (Detener eventos de anotaciones)
Utilice este mandato para dejar de anotar los eventos en un receptor activo.
- EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)
Utilice este mandato para iniciar manualmente el proceso de caducidad de inventario. El proceso de caducidad de inventario elimina las copias de los archivos de archivado y de copia de seguridad de cliente del almacenamiento del servidor. La eliminación se basa en las especificaciones de política de los grupos de copia de archivado y de copia de seguridad y archivo de las clases de gestión a las que están vinculados los archivos.
- Mandatos EXPORT
Utilice el mandato EXPORT para copiar información de un servidor de IBM Spectrum Protect en un medio extraíble secuencial.
- EXTEND DBSPACE (Incrementar el espacio para la base de datos)
Utilice este mandato para aumentar el espacio para la base de datos añadiendo directorios para que los utilice la base de datos.
- Mandatos GENERATE
Utilice los mandatos GENERATE para los conjuntos de copia de seguridad para un espacio de archivos o un nodo cliente seleccionado.
- Mandatos GRANT
Utilice el mandato GRANT para otorgar el acceso o los privilegios apropiados.
- HALT (Concluir el servidor)
Utilice este mandato para concluir el servidor. El mandato HALT fuerza una conclusión precipitada, que cancela todas las sesiones de nodo cliente y de administración, aunque no se hayan completado.
- HELP (Obtener ayuda sobre mandatos y mensajes de error)
Utilice este mandato para visualizar los mandatos de administración y los mensajes de error. Puede emitir el mandato desde un cliente de línea de mandatos de administración.
- IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)
Utilice este mandato para iniciar o detener procesos que identifiquen datos duplicados en una agrupación de almacenamiento. Puede especificar el número de proceso de identificación de duplicados y su duración.
- Mandatos IMPORT
Utilice los mandatos IMPORT para importar información desde los medios de exportación a un servidor de IBM Spectrum Protect.
- INSERT MACHINE (Insertar información de características o instrucciones de recuperación)
Utilice este mandato para agregar características de máquina cliente o instrucciones de recuperación a la información de la máquina existente en la base de datos.
- ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)
Utilice este mandato con el proceso de código de retorno en un script para emitir un mensaje desde un script del servidor para determinar dónde se encuentra el problema con un mandato del script.
- LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
Utilice este mandato para etiquetar volúmenes de cinta o, en una biblioteca automatizada, para etiquetar automáticamente los volúmenes a medida que se dan de alta. Con este mandato, servidor utiliza la etiqueta larga que, con frecuencia, los volúmenes llevan previamente etiquetada.
- LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)
Utilice este mandato para cargar el conjunto predeterminado de desencadenantes de alertas en el servidor de IBM Spectrum Protect.
- Mandatos LOCK
Utilice el mandato LOCK para impedir que los usuarios accedan al servidor.
- MACRO (Invocar una macro)
Utilice este mandato para invocar un archivo desde la línea de mandatos de administración que contiene uno o varios mandatos de administración de IBM Spectrum Protect que deben ejecutarse.
- MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)
Utilice este mandato para migrar archivos de una agrupación de almacenamiento a la agrupación de almacenamiento siguiente de la jerarquía de almacenamiento.
- Mandatos MOVE
Utilice los mandatos MOVE para transferir datos de copia de seguridad o datos archivados entre agrupaciones de almacenamiento o bien para trasladar medios de recuperación ante siniestro al local o fuera del local.
- NOTIFY SUBSCRIBERS (Notificar a servidores gestionados que actualicen los perfiles)
Utilice este mandato en un gestor de configuración para notificar a uno o varios servidores gestionados que soliciten que su información de configuración se renueve inmediatamente.
- PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca)
Utilice este mandato para definir o suprimir todas las unidades y sus rutas para una única biblioteca en un paso.
- PING SERVER (Comprobar la conexión entre servidores)
Utilice este mandato para comprobar la conexión entre el servidor local y un servidor remoto.

- **PREPARE** (crear un archivo de plan de recuperación)
Utilice este mandato para crear un archivo de plan de recuperación, que contiene la información necesaria para recuperar un servidor de IBM Spectrum Protect. El archivo del plan de recuperación se puede almacenar en un sistema de archivos que sea accesible para el servidor de origen o en un servidor de destino.
- **PROTECT STGPOOL** (Proteger datos que pertenecen a una agrupación de almacenamiento)
Utilice este mandato para proteger los datos de una agrupación de almacenamiento de contenedores de directorio almacenando una copia de los datos en otra agrupación de almacenamiento en un servidor de destino de duplicación o en el mismo servidor protegiendo los datos en cinta. Cuando protege la agrupación de almacenamiento de contenedores de directorio, puede intentar posteriormente reparar los daños en la agrupación de almacenamiento mediante el mandato REPAIR STGPOOL.
- **Mandatos QUERY**
Utilice los mandatos QUERY para solicitar o visualizar información sobre los objetos de IBM Spectrum Protect.
- **QUIT** (finalizar la modalidad interactiva del cliente de administración)
Utilice este mandato para finalizar una sesión de cliente de administración en modalidad interactiva.
- **RECLAIM STGPOOL** (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)
Utilice este mandato para reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial. La reclamación no traslada las versiones inactivas de los datos de copia de seguridad de los volúmenes en las agrupaciones de datos activos.
- **RECONCILE VOLUMES** (Reconciliar diferencias en definiciones de volúmenes virtuales)
Emita este mandato desde el servidor de origen para reconciliar las diferencias que hay entre las definiciones de volúmenes virtuales del servidor de origen y las copias archivadas del servidor de destino. IBM Spectrum Protect localiza todos los volúmenes de la clase de dispositivo especificada del servidor de origen y todas las copias archivadas correspondientes del servidor de destino. El inventario del servidor de destino también se compara con la definición local de los volúmenes virtuales para ver si existen incoherencias.
- **Mandatos REGISTER**
Utilice los mandatos REGISTER para definir o agregar objetos para IBM Spectrum Protect.
- **Mandatos REMOVE**
Utilice los mandatos REMOVE para eliminar un objeto de IBM Spectrum Protect.
- **Mandatos RENAME**
Utilice los mandatos RENAME para cambiar el nombre de un objeto existente.
- **REPAIR STGPOOL** (Reparar una agrupación de almacenamiento de contenedores de directorio)
Utilice este mandato para reparar extensiones con duplicados eliminados en una agrupación de almacenamiento de contenedores de directorio. Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones de las que se ha hecho copia de seguridad en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.
- **REPLICATE NODE** (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)
Utilice este mandato para replicar los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, o a grupos definidos de nodos de clientes.
- **REPLY** (Permitir una petición para continuar el proceso)
Utilice este mandato y un número de identificación para informar al servidor de que ha finalizado una operación solicitada. No todas las peticiones de servidor requieren una respuesta. Este mandato sólo es necesario si el mensaje de petición indica específicamente que se necesita una respuesta.
- **RESET PASSEXP** (restablecer caducidad de contraseña)
Utilice el mandato RESET PASSEXP para restablecer el período de caducidad de las contraseñas en el período de caducidad común para las contraseñas de administrador y de nodo de cliente. El mandato RESET PASSEXP no se aplica a las contraseñas que se almacenan en un servidor de directorios LDAP.
- **RESTART EXPORT** (Reiniciar una operación de exportación suspendida)
Utilice este mandato para reiniciar una operación de exportación suspendida.
- **Mandatos RESTORE**
Utilice los mandatos RESTORE para restaurar las agrupaciones de almacenamiento o volúmenes IBM Spectrum Protect.
- **Mandatos REVOKE**
Utilice los mandatos REVOKE para revocar el acceso o los privilegios.
- **ROLLBACK** (Retrotraer cambios no validados en una macro)
Utilice este mandato en una macro para deshacer todos los cambios de proceso que han realizado los mandatos que el servidor ha ejecutado pero que todavía no se han validado en la base de datos. Un cambio validado es permanente y no se puede retrotraer. El mandato ROLLBACK es útil para probar las macros.
- **RUN** (ejecutar un script de IBM Spectrum Protect)
Utilice este mandato para ejecutar un script de IBM Spectrum Protect. Para emitir este mandato en otro servidor, el script que se ejecuta debe estar definido en ese servidor.
- **SELECT** (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)
Utilice el mandato SELECT para crear y dar formato a una consulta personalizada de la base de datos de IBM Spectrum Protect .
- **Mandatos SET**
Utilice los mandatos SET para especificar valores que afectan a varias operaciones de IBM Spectrum Protect.
- **SETOPT** (Establecer una opción de servidor para actualización dinámica)
Puede utilizar el mandato SETOPT para actualizar la mayoría de las opciones de servidor dinámicamente sin detener y reiniciar

el servidor. Para la opción DBDIAGLOGSIZE, debe detener e iniciar el servidor. Un mandato SETOPT que esté en una macro o en un script no se puede retrotraer.

- SHRED DATA (destruir datos)
Utilice este mandato para iniciar manualmente el proceso de destrucción de los datos confidenciales suprimidos. La destrucción manual de datos es posible únicamente si la destrucción automática está inhabilitada.
- SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)
Utilice este mandato para suspender una operación de exportación de servidor a servidor que tiene un valor de FILEDATA que no es NONE. La operación de exportación que desea suspender debe haber pasado la fase de inicialización para poder considerarse seleccionable para la suspensión. El estado de la operación de exportación se guarda. La operación puede reiniciarse mediante la emisión del mandato RESTART EXPORT.
- Mandatos UNLOCK
Utilice los mandatos UNLOCK para restablecer el acceso después de que se haya bloqueado un objeto.
- Mandatos UPDATE
Utilice el mandato UPDATE para modificar uno o más atributos de un objeto IBM Spectrum Protect existente.
- Mandatos VALIDATE
Utilice el mandato VALIDATE para verificar que un objeto esté completo o sea válido para IBM Spectrum Protect.
- VARY (Activar o desactivar un volumen de acceso aleatorio)
Utilice este mandato para activar o desactivar un volumen de agrupación de almacenamiento de acceso aleatorio en el servidor.

ACCEPT DATE (aceptar la fecha del sistema actual)

Utilice este mandato para que el servidor pueda iniciar un proceso normal, cuando el servidor no inicia un proceso normal a causa de una discrepancia entre la fecha del servidor y la fecha actual del sistema.

Cuando el servidor no comienza el proceso normal debido a una discrepancia entre la fecha del servidor y la fecha actual, este mandato obliga al servidor a aceptar la fecha y hora actuales como válidas. Si la hora del sistema es válida y el servidor no se ha ejecutado durante cierto tiempo, este mandato debería ejecutarse para permitir el comienzo del proceso normal del servidor.

Atención: Si la fecha del sistema no es válida o el servidor se creó o se ejecutó previamente con una fecha del sistema no válida y se emite este mandato, cualquier proceso del servidor o mandato que utilice fechas puede tener resultados imprevistos. Por ejemplo, la caducidad de los archivos puede verse afectada. Cuando el servidor se inicia con la fecha correcta, los archivos con copias de seguridad con fecha en el futuro no serán consideradas para caducidad hasta que se alcance la fecha futura. Los archivos con copias de seguridad con fechas que han pasado caducarán antes. Cuando el proceso del servidor detecta una fecha futura, se emitirá un mensaje de error.

Si el servidor detecta una fecha u hora no válidas, las sesiones del servidor se inhabilitarán (como si se hubiera emitido el mandato DISABLE SESSIONS). No se pueden continuar procesando las operaciones de caducidad, migración, reclamación y supresión de información histórica de volúmenes.

Utilice el mandato ENABLE SESSIONS ALL después de haber emitido el mandato ACCEPT DATE para volver a habilitar las sesiones que han de iniciarse.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-ACcEpt Date-----<<
```

Parámetros

Ninguno.

Ejemplo: aceptar la fecha del sistema actual

Permitir que el servidor acepte la fecha actual como la fecha válida.

```
accept date
```

Mandatos relacionados

Tabla 1. Mandato relacionado con ACCEPT DATE

Mandato	Descripción
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.

ACTIVATE POLICYSET (Activar un nuevo juego de políticas)

Utilice este mandato para copiar el contenido de un juego de políticas en el juego de políticas ACTIVE del dominio. El servidor utiliza las reglas del juego de políticas ACTIVE para gestionar las operaciones de cliente en el dominio. Puede definir varios juegos de políticas para un dominio de políticas, pero únicamente puede haber un juego de políticas activo. El juego de políticas ACTIVE actual se sustituye por el que especifique al emitir este mandato. Sólo puede modificar el juego de políticas ACTIVE activando otro juego de políticas.

Antes de activar un juego de políticas, compruebe que el juego de políticas está completo y es válido con el mandato VALIDATE POLICYSET.

El mandato ACTIVATE POLICYSET no se ejecutará correctamente si se da alguna de las condiciones que se indican a continuación:

- Un grupo de copia especifica una agrupación de almacenamiento de copia como destino.
- Una clase de gestión especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.
- El juego de políticas no tiene ninguna clase de gestión predeterminada.
- Se ha especificado un parámetro TOCDESTINATION y la agrupación de almacenamiento es una agrupación de copia o bien tiene un formato de datos distinto de NATIVE o NONBLOCK.

El juego de políticas ACTIVE y el último juego de políticas activado no son necesariamente idénticos. Puede modificar el juego de políticas original que ha activado sin que afecte al juego de políticas ACTIVE.

Si el servidor tiene la protección de retención de datos activada, deben darse las condiciones siguientes:

- Todas las clases de gestión del juego de políticas que se va a activar deben contener un grupo de copia archivada.
- Si existe una clase de gestión en el juego de políticas activo, debe existir una clase de gestión con el mismo nombre en el juego de políticas que se va a activar.
- Si existe un grupo de copia archivada en el juego de políticas activo, el grupo de copia correspondiente en el juego de políticas que se va a activar debe tener un valor de RETVER que sea por lo menos tan alto como los valores correspondientes en el grupo de copia activo.

Atención: La protección de retención sólo se aplica a los objetos de archivado.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-ACTivate Policyset--nombre_dominio--nombre_juego_políticas--><
```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas para el que desea activar un juego de políticas.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas que se va a activar.

Ejemplo: activar un juego de políticas en un dominio de políticas específico

Activar el juego de políticas VACATION en el dominio de políticas EMPLOYEE_RECORDS.

```
activate policyset employee_records vacation
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ACTIVATE POLICYSET

Mandato	Descripción
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

ASSIGN DEFMGMTCLASS (asignar una clase de gestión predeterminada)

Utilice este mandato para especificar una clase de gestión como la clase de gestión predeterminada para un juego de políticas. Para poder activar el juego de políticas, debe asignar una clase de gestión predeterminada a un juego de políticas.

Para garantizar que los clientes siempre podrán realizar la copia de seguridad y las copias archivadas, seleccione una clase de gestión predeterminada que contenga un grupo de copia archivada y un grupo de copia de seguridad.

El servidor utiliza la clase de gestión predeterminada para gestionar los archivos de cliente si no hay ninguna clase de gestión asignada o adecuada. Por ejemplo, el servidor utiliza la clase de gestión predeterminada si el usuario no especifica una clase de gestión en la lista de inclusión/exclusión.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-ASSign DEFMGmtclass--nom_dominio--nom_juego_políticas--nom_clase-><
```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas para el que desea asignar una clase de gestión predeterminada. No puede asignar una clase de gestión predeterminada al juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica la clase de gestión que será la clase de gestión predeterminada para el juego de políticas.

Ejemplo: asignar una clase de gestión predeterminada

Asignar DEFAULT1 como la clase de gestión predeterminada para el juego de políticas SUMMER del dominio de políticas PROG1.

```
assign defmgmtclass prog1 summer default1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ASSIGN DEFMGMTCLASS

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.

Mandato	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

Mandatos AUDIT

Utilice los mandatos AUDIT para revisar o examinar si tanto la información de la base de datos como el volumen de agrupación de almacenamiento están en un estado correcto. El mandato AUDIT LDAPDIRECTORY elimina los nodos o ID de administrador de un servidor de directorio LDAP, que no autentican sus contraseñas con el servidor de directorio LDAP.

- AUDIT CONTAINER
 - AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)
 - AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)
- AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)
- AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)
- AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)
- AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Mandatos AUDIT CONTAINER

Utilice el mandato AUDIT CONTAINER para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes.

- AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)
Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.
- AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)
Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de directorio.

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)

Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.

Puede utilizar este mandato para realizar las siguientes acciones para un contenedor de una agrupación de almacenamiento de contenedores de nubes:

- Explorar el contenido de un contenedor para validar la integridad de las extensiones de datos

- Eliminar datos de un contenedor marcado como *dañado*, como por ejemplo cuando un archivo tiene referencias en la base de datos del servidor, pero contiene datos faltantes o corrompidos en la nube.
- Marcar un contenedor completo como dañado
- Eliminar datos marcados como *huérfanos*, como por ejemplo cuando un objeto almacenado en la nube no tiene una referencia en la base de datos del servidor

Clase de privilegio

Para utilizar este mandato, debe tener privilegios de sistema o privilegios de almacenamiento sin restricciones.

Sintaxis

```
>>-AUDit CONTainer--+-nombre_contenedor-----+-->
      +-STGpool---nombre_agrupación-----+
      '-STGpool---nombre_agrupación--STGPOOLDIrectory---nombre_directorio-'

.-Action----SCANAll-----.
>+-----+-----+-----+-----+-----+----->
  '-Action---+-SCANAll-----+'
            +-REMOVEDamaged-+
            +-MARKDamaged---+
            '-SCANDamaged--'

.-FORCEOrphanbdel----No-----.
>+-----+-----+-----+-----+-----+----->
  '-FORCEOrphanbdel----+No--+'
                        '-Yes-'

.-MAXProcess----4-----.-Wait----No-----.
>+-----+-----+-----+-----+-----+----->
  '-MAXProcess----número-' '-Wait----+No--+'
                                  '-Yes-'

.-BEGINdate----antes_primera_auditoría-.
>+-----+-----+-----+-----+-----+----->
  '-BEGINdate----fecha_inicio-----'

.-BEGINTime----00:00:00----.
>+-----+-----+-----+-----+-----+----->
  '-BEGINTime----hora_inicio-'

.-ENDDate----después_última_auditoría-.
>+-----+-----+-----+-----+-----+----->
  '-ENDDate----fecha_final-----'

.-ENDTime----23:59:59-----.
>+-----+-----+-----+-----+-----+-----><
  '-ENDTime----hora_finalización-'
```

Parámetros

nombre_contenedor

Especifica el nombre del contenedor que desea auditar. Si no especifica este parámetro, debe especificar una agrupación de almacenamiento de contenedores de nubes.

STGpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de nubes que desea auditar. Este parámetro es opcional. Si sólo especifica este parámetro, se auditan todos los contenedores definidos para la agrupación de almacenamiento. Si no especifica este parámetro, debe especificar un contenedor.

STGPOOLDIrectory

Especifica el nombre del directorio de la agrupación de almacenamiento de contenedor en la nube que desea auditar. Este parámetro es opcional.

Restricción: debe especificar una agrupación de almacenamiento que utilice almacenamiento local.

Acción

Especifica la acción que realizará el servidor cuando se realiza la auditoría de un contenedor de una agrupación de almacenamiento de contenedores de nubes. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

SCANAll

Especifica que el servidor identifica los registros de base de datos que hacen referencia a las extensiones de datos con incoherencias. Se efectúa una marca para los datos de la agrupación de almacenamiento de contenedor en la nube que no coinciden con los datos de la base de datos del servidor. Este es el valor predeterminado. El servidor marca la extensión de datos como dañada en la base de datos.

Consejo: Si especifica el parámetro ACTION=SCANALL en una agrupación de almacenamiento IBM® Cloud Object Storage que utiliza una cámara de seguridad con la indexación de nombres inhabilitada, la operación de auditoría explora toda la cámara de seguridad para identificar extensiones huérfanas en cada contenedor. En esta situación, especifique WAIT=YES si desea que la operación de auditoría espere a que finalice la exploración de extensiones huérfanas antes de que notifique la auditoría como completada. Esta exploración de extensiones huérfanas sólo se produce si no se especifica un nombre de contenedor. Si especifica un contenedor que se encuentra en una cámara de seguridad con la indexación de nombres inhabilitada, la operación de auditoría no explora extensiones huérfanas.

REMOVEDamaged

Especifica que el servidor elimina cualquier referencia a extensiones dañadas de la base de datos de servidor. Las extensiones dañadas también se eliminan de la agrupación de almacenamiento del contenedor de la nube, si se han encontrado. El servidor también elimina las extensiones huérfanas de la agrupación de almacenamiento de contenedor en la nube y elimina las referencias a estas extensiones huérfanas de la base de datos, según especifica el parámetro FORCEORPHANDBDEL.

MARKDamaged

Especifica que el servidor marca explícitamente todas las extensiones de datos en el contenedor como dañadas.

SCANDamaged

Especifica que el servidor sólo comprueba las extensiones dañadas existentes en el contenedor.

Importante: si no existe ninguna conexión con la nube, los parámetros ACTION=SCANALL y ACTION=SCANDAMAGED no se ejecutan. Sin embargo, el parámetro ACTION=MARKDAMAGED se ejecuta según lo esperado sin conexión de nube, y el parámetro ACTION=REMOVEDAMAGED marca los datos dañados como huérfanos. En cuanto se restablece la conexión con la nube, el servidor suprime las extensiones huérfanas.

Condición de restablecimiento de estado: Si la auditoría no detecta un error con una extensión de datos marcada como dañada, el estado de la extensión de datos se restablece. A continuación, la extensión de datos puede utilizarse. Esta condición proporciona un medio de restablecer el estado de las extensiones de datos dañadas si los errores se deben a un problema corregible. Las opciones SCANALL y SCANDAMAGED son las únicas opciones que restablecen una extensión dañada si se descubre que no está dañadas.

FORCEOrphandbdel

Especifica que el servidor fuerza la supresión de extensiones huérfanas de la base de datos del servidor, aunque no se hayan suprimido de la agrupación de almacenamiento del contenedor de la nube. Este parámetro es opcional. Si especifica este parámetro, también debe especificar el parámetro ACTION=REMOVEDAMAGED. Las opciones siguientes están disponibles:

Yes

Especifica que el servidor suprime cualquier extensión huérfana de la base de datos del servidor, aunque no se hayan suprimido de la agrupación de almacenamiento del contenedor de la nube.

No

Especifica que el servidor conserva las extensiones huérfanas en la base de datos del servidor, si no se pueden suprimir de la agrupación de almacenamiento del contenedor de la nube. Este es el valor predeterminado.

MAXProcess

Especifica el número de procesos paralelos que se utilizarán para comprobar un contenedor en una agrupación de almacenamiento de contenedores de nubes. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

Restricción: El servidor omite este parámetro cuando se utiliza MAXPROCESS con el parámetro ACTION=REMOVEDAMAGED.

Wait

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras el mandato se está procesando. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se muestran en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.

BEGINDate

Especifica el valor del rango de fechas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no una fecha inicial, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha antes de que se realizara la primera auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para auditar todos los contenedores que se auditaron la semana pasada, especifique BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

BEGINTime

Especifica el valor del rango de horas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado es 00:00:00. Si no especificó un rango de fechas, el valor predeterminado es la fecha de hoy. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	10:30:08
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-04:00 o -04:00. Si emite este mandato a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect audita contenedores cuya última hora de auditoría sea las 5:30 o posterior en la fecha inicial.

ENDDate

Especifica el valor del rango de fechas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no un valor, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha después de que se realizara la última auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para incluir contenedores auditados hasta ayer, puede especificar ENDDATE=TODAY-1 o ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

ENDTime

Especifica el valor del rango de horas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado son las 23:59:59. Este parámetro es opcional.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	10:30:08
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o anterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, se auditan los contenedores cuya última hora de auditoría sea las 5:30 o anterior en la fecha final especificada.

Ejemplo: auditar un contenedor específico en una agrupación de almacenamiento de contenedor de nubes

Audite el contenedor 42-00000my000example000container000 de la agrupación de almacenamiento de contenedor de nubes.

```
audit container 42-00000my000example000container000 action=scanall
```

Ejemplo: auditar una agrupación de almacenamiento de contenedores de nubes en un marco de tiempo específico

Auditar una agrupación de almacenamiento de contenedores de nubes llamada POOL3 e incluir solamente los contenedores de ayer entre las 9:30 y las 12:30.

```
audit container stgpool=pool3 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabla 1. Mandatos relacionados con AUDIT CONTAINER

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.

STGPOOLDirectory

Especifica el nombre del directorio de agrupación de almacenamiento de contenedores que desea auditar. Este parámetro es opcional. Si especifica este parámetro, se auditan todos los contenedores definidos en el directorio de agrupación de almacenamiento de contenedores. Para especificar este parámetro, también debe especificar una agrupación de almacenamiento.

Acción

Especifica la acción que realizará el servidor cuando se realiza la auditoría de un contenedor de una agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

SCANAll

Especifica que el servidor identifica los registros de base de datos que hacen referencia a las extensiones de datos con incoherencias. Este es el valor predeterminado. El servidor marca la extensión de datos como dañada en la base de datos. Consejo: Si ha utilizado el mandato PROTECT STGPOOL en una agrupación de almacenamiento de contenedores de directorio en el servidor de destino, puede reparar la extensión de datos dañada utilizando el mandato REPAIR STGPOOL.

REMOVEDamaged

Especifica que el servidor elimina los archivos de la base de datos que hagan referencia a la extensión de datos dañada.

MARKDamaged

Especifica que el servidor marca explícitamente todas las extensiones de datos en el contenedor como dañadas.

SCANDamaged

Especifica que el servidor sólo comprueba las extensiones dañadas existentes en el contenedor.

Condición de restablecimiento de estado: Si la auditoría no detecta un error con una extensión de datos marcada como dañada, el estado de la extensión de datos se restablece. A continuación, la extensión de datos puede utilizarse. Esta condición proporciona un medio de restablecer el estado de las extensiones de datos dañadas si los errores se deben a un problema corregible. Las opciones SCANALL y SCANDAMAGED son las únicas opciones que restablecen una extensión dañada si se descubre que no está dañada.

MAXProcess

Especifica el número de procesos paralelos que se utilizarán para comprobar un contenedor en una agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

Wait

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras el mandato se está procesando. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se muestran en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.

BEGINDate

Especifica el valor del rango de fechas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no una fecha inicial, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha antes de que se realizara la primera auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para auditar todos los contenedores que se auditaron la semana pasada, especifique BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

BEGINTime

Especifica el valor del rango de horas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado es 00:00:00. Si no especificó un rango de fechas, el valor predeterminado es la fecha de hoy. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	10:30:08
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-04:00 o -04:00. Si emite este mandato a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect audita contenedores cuya última hora de auditoría sea las 5:30 o posterior en la fecha inicial.

ENDDate

Especifica el valor del rango de fechas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no un valor, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha después de que se realizara la última auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para incluir contenedores auditados hasta ayer, puede especificar ENDDATE=TODAY-1 o ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM

Valor	Descripción	Ejemplo
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

ENDTime

Especifica el valor del rango de horas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado son las 23:59:59. Este parámetro es opcional.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	10:30:08
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o anterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, se auditan los contenedores cuya última hora de auditoría sea las 5:30 o anterior en la fecha final especificada.

Ejemplo: auditar un contenedor de agrupación de almacenamiento determinado

Audite el contenedor de agrupación de almacenamiento 0000000000000721.dcf.

```
audit container n:\ddcont2\07\0000000000000721.dcf action=scanall
```

Ejemplo: Eliminar los datos dañados de una agrupación de almacenamiento de contenedores de directorio

Auditar una agrupación de almacenamiento de contenedores de directorio llamada NEWDEDUP y eliminar los archivos dañados.

```
audit container stgpool=newdedup action=removedamaged
```

Ejemplo: Marcar como dañados todos los datos de una agrupación de almacenamiento de contenedores de directorio

Auditar una agrupación de almacenamiento de contenedores de directorio llamada NEWDEDUP y marcar todos los archivos como dañados.

```
audit container stgpool=newdedup maxprocess=2 action=markdamaged
```

Ejemplo: auditar una agrupación de almacenamiento de contenedores de directorios en un marco de tiempo específico

Auditar una agrupación de almacenamiento de contenedores de directorios llamada POOL2 e incluir solamente los contenedores anteriores a ayer entre las 9:30 y las 12:30.

```
audit container stgpool=pool2 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabla 1. Mandatos relacionados con AUDIT CONTAINER

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.

Mandato	Descripción
MOVE CONTAINER	Mueve el contenido de un contenedor de agrupación de almacenamiento a otro contenedor.
QUERY DAMAGED	Muestra información sobre los archivos dañados.

AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)

Utilice este mandato para auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de LDAP (Lightweight Directory Access Protocol). El servidor LDAP y el espacio de nombres se especifican mediante una o varias opciones LDAPURL.

Restricción: Utilice este mandato únicamente si ha configurado la autenticación de contraseña, como se describe en la sección Autenticación de los usuarios mediante un servidor LDAP. La información que se proporciona acerca del mandato AUDIT LDAPDIRECTORY únicamente se aplica a los entornos en los que la autenticación de contraseña se ha configurado como se describe en la sección Autenticación de los usuarios mediante un servidor LDAP.

Los nodos y los ID de usuario administrador que no autentican sus contraseñas con el servidor de directorios LDAP se suprimen con el mandato AUDIT LDAPDIRECTORY FIX=YES . Los nodos e ID de usuario administrador que ya no existen en la base de datos de IBM Spectrum Protect también se eliminan.

Antes de emitir este mandato, asegúrese de que se especifica la opción LDAPURL en el archivo dsmserv.opt . Consulte la opción LDAPURL para obtener más información. Si especificó más de una opción LDAPURL en el archivo dsmserv.opt , cada opción está válida en el orden en el que se colocaron. Si la opción LDAPURL no está especificada, el mandato falla.

Clase de privilegio

Para emitir este mandato, debe tener privilegios de sistema.

Sintaxis

```

.-Fix-----No----- .
>>-AUDIT LDAPdirectory----->
'-Fix-----+No---+'
'-Yes-'

.-Wait-----No----- .
>----->
'-Wait-----+No---+'
'-Yes-'

```

Parámetros

Fix

Este parámetro opcional especifica cómo el servidor de IBM Spectrum Protect resuelve las incoherencias entre la base de datos y el directorio externo. El valor predeterminado es NO. Puede especificar los siguientes valores:

No

El servidor informa de todas las incoherencias, pero no cambia el directorio externo.

Yes

El servidor resuelve las inconsistencias que puede y sugiere más acciones, si es necesario.

Importante: Si hay entradas LDAP que se comparten con otros servidores de IBM Spectrum Protect, la selección YES puede hacer que esos servidores dejen de estar sincronizados.

Wait

Este parámetro opcional especifica si se ha de esperar a que el servidor de IBM Spectrum Protect complete el proceso de este mandato de forma subordinada. El valor predeterminado es NO. Puede especificar los siguientes valores:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Yes

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: Auditar un directorio LDAP y reparar las incoherencias

Realice una auditoría del directorio LDAP que ha especificado en la opción LDAPURL. El servidor IBM Spectrum Protect resuelve algunas inconsistencias.

```
audit ldapdirectory fix=yes
```

```
ANR2749W El administrador ADMIN1 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2749W El administrador ADMIN2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2749W El nodo NODE1 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2749W El nodo NODE2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2748W El nodo NODE1 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2748W El nodo NODE2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.
ANR2745I Se ha completado el mandato AUDIT LDAPDIRECTORY: solo hay 4 entradas del administrador de nodo en el servidor de directorio LDAP (no en el servidor de IBM Spectrum Protect), solo hay 0 entradas de administrador en el servidor de IBM Spectrum Protect (no en el servidor de directorio LDAP), solo hay 2 entradas de nodo en el servidor de directorio LDAP (no en el servidor de IBM Spectrum), solo hay 0 entradas de nodo en el servidor de IBM Spectrum Protect, (no en el servidor de directorio LDAP), 6 entradas se han suprimido del servidor LDAP en total.
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con AUDIT LDAPDIRECTORY

Mandato	Descripción
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.

AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)

Utilice este mandato para auditar y sincronizar inventarios de volúmenes en una biblioteca automatizada.

Cuando se emite el mandato AUDIT LIBRARY en un cliente de biblioteca, el cliente sincroniza su inventario con el inventario del gestor de bibliotecas. Si el cliente de biblioteca detecta incongruencias, las corrige por medio de un cambio en la propiedad del volumen en el gestor de biblioteca.

Cuando se emite el mandato AUDIT LIBRARY en un servidor en el que la biblioteca es SCSI, 349X o ACSLS (LIBTYPE=SCSI, LIBTYPE=349X o LIBTYPE=ACSL), el servidor sincroniza su inventario con el inventario del dispositivo de bibliotecas. Si el servidor detecta incoherencias, elimina los volúmenes ausentes de su inventario.

- En las bibliotecas SCSI, el servidor actualiza también las ubicaciones de los volúmenes de su inventario que han sido trasladados desde la última auditoría.
- En las bibliotecas 349X, el servidor garantiza también que los volúmenes reutilizables se encuentran en la categoría reutilizable y los volúmenes privados en la categoría privada.

Cuando se emite el mandato AUDIT LIBRARY en un servidor que es un gestor de bibliotecas de la biblioteca (SHARED=YES), el servidor actualiza la propiedad de sus volúmenes si detecta incoherencias.

Con independencia del servidor o del tipo de biblioteca, la emisión del mandato AUDIT LIBRARY no agrega automáticamente nuevos volúmenes a una biblioteca. Para agregar nuevos volúmenes, debe utilizar el mandato CHECKIN LIBVOLUME.

Atención: Las siguientes precauciones son aplicables sólo a las bibliotecas SCSI, 349X y ACSLS (LIBTYPE=SCSI, LIBTYPE=349X y LIBTYPE=ACSL):

- La ejecución del mandato AUDIT LIBRARY impide que tenga lugar cualquier otra actividad de biblioteca hasta que se ha completado la auditoría. Por ejemplo, el servidor no procesará, restaurará ni recuperará peticiones que impliquen a la biblioteca cuando esté ejecutándose el mandato AUDIT LIBRARY.
- Si está realizándose cualquier otra actividad en la biblioteca, no emita el mandato AUDIT LIBRARY. La emisión del mandato AUDIT LIBRARY cuando una biblioteca está activa puede producir resultados imprevisibles (por ejemplo, una condición de bloqueo) si un proceso que está accediendo actualmente a la biblioteca intenta adquirir un nuevo montaje de cinta.

Este mandato crea un proceso subordinado que puede cancelar con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-AUDIT LIBRARY--nombre_biblioteca----->
. -CHECKLabel---Yes-----
>--+-----+----->
' -CHECKLabel---+Yes---+'
      '-Barcode-'

. -REFRESHstate---No-----
>--+-----+----->>
' -REFRESHstate---+No---+'
      '-Yes-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de auditar.

CHECKLabel

Especifica cómo se comprueba la etiqueta del volumen de almacenamiento durante el proceso de auditoría. Este parámetro sólo se aplica a las bibliotecas SCSI. Este parámetro se pasa por alto en otros tipos de bibliotecas. El valor predeterminado es YES.

Los valores posibles son:

Yes

Especifica que el servidor comprueba cada etiqueta de volumen para verificar la identidad del volumen.

Barcode

Especifica que el servidor utiliza el lector de códigos de barra para leer la etiqueta de almacenamiento. Al utilizar códigos de barras, el tiempo de proceso de la auditoría disminuye. Este parámetro sólo se aplica a las bibliotecas SCSI.

Atención: Si el escáner no puede leer una etiqueta de código de barras determinada, o si falta una etiqueta de código de barras, el servidor carga esa cinta en una unidad para leer la etiqueta.

REFRESHstate

Especifica si la información del servidor sobre una biblioteca, que normalmente se obtiene durante la inicialización, se renueva para que se reflejen los cambios en la configuración. Si se establece el parámetro REFRESHSTATE en Yes, esta acción se realiza sin necesidad de reiniciar el servidor o redefinir la biblioteca. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor no actualiza el estado de la biblioteca al auditar esta.

Yes

Especifica que el servidor no actualiza el estado de la biblioteca cuando se emite el mandato AUDIT LIBRARY.

Ejemplo: auditar una biblioteca automatizada

Mandatos relacionados

Tabla 1. Mandatos relacionados con AUDIT LIBRARY

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE LIBRARY	Suprime una biblioteca.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)

Utilice este mandato para determinar si un volumen de cinta está intacto y para auditar datos en cualquier volumen de cinta.

Puede emitir el mandato AUDIT LIBVOLUME desde cualquier volumen de cinta que está incorporado en una biblioteca. El mandato se ejecuta en segundo plano de forma predeterminada. Puede emitir el mandato desde los tipos de bibliotecas siguientes que tienen unidades IBM® TS1140, IBM LTO 5 o una unidad de cintas de generación posterior:

- biblioteca de cintas SCSI
- Biblioteca virtual de cintas (VTL)

La tabla siguiente describe las unidades de cinta que pueden verificar volúmenes de cinta con tipos de soporte para unidades de cinta de IBM TS1140 y IBM LTO 5 y una generación posterior de LTO:

Tabla 1. Unidades de cinta y tipos de soporte

Unidad	Tipo de medio
TS1140	JB, JX, JA, JW, JJ, JR, JC, JY y JK
IBM LTO 5	LTO 3, LTO 4 y LTO 5
IBM LTO 6	LTO 4, LTO 5 y LTO 6
IBM LTO 7	LTO 5, LTO 6 y LTO 7

La tabla siguiente describe el nivel mínimo de controlador de dispositivo que se requiere para ejecutar el mandato:

Tabla 2. Nivel mínimo de controlador de dispositivo de IBM

Nombre de controlador	Nivel de controlador de dispositivo
Controlador Atape en AIX	12.3.5.00
controlador lin_tape en Linux	1.6.7.00
Controlador de cintas de IBM en Windows	6.2.2.00

Restricción: No puede emitir el mandato CANCEL PROCESS mientras el mandato AUDIT LIBVOLUME está en curso.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones para la biblioteca en la que se ha definido el volumen de cinta.

Sintaxis


```
>>-AUDit LIBVolume--nombre_biblioteca--nombre_volumen----->
      .-Wait---No-----.
>+-----+-----><
      '-Wait---No---+'
          '-Yes-'
```

Parámetros

nombre_biblioteca (necesario)

Especifica el nombre del volumen de biblioteca donde está ubicado el volumen de cinta que desea auditar.

nombre_volumen (necesario)

Especifica el nombre del volumen de cinta físico que desea auditar.

Wait (Opcional)

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

No

Especifica que la operación se ha completado en segundo plano. El valor NO es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse.

Ejemplo: Auditar un volumen de cinta

Audite la biblioteca EZLIFE que tiene un volumen de cinta que se denomina KM0347L5.

```
audit libvolume ezlife KM0347L5
```

AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)

Utilice este mandato para hacer la auditoría del almacenamiento del servidor que utilizan los nodos cliente y la de las licencias del servidor. La auditoría determina si la configuración actual es conforme a los plazos de licencia.

Una auditoría crea un proceso subordinado que puede cancelar con el mandato CANCEL PROCESS. Si detiene el servidor y vuelve a iniciarlo, se ejecutará automáticamente una auditoría, tal como especifica el mandato SET LICENSEAUDITPERIOD. Para ver los resultados de la auditoría, utilice el mandato QUERY LICENSE.

Atención: La auditoría del almacenamiento del servidor puede emplear una gran cantidad de tiempo de CPU. Puede utilizar la opción del servidor AUDITSTORAGE para especificar que no se haga la auditoría del almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-AUDit LICenses-----><
```

Parámetros

Ninguno.

Ejemplo: auditar licencias de servidor

Emitir el mandato AUDIT LICENSES.

```
audit licenses
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con AUDIT LICENSES

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY AUDIT OCCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
SET LICENSE AUDIT PERIOD	Especifica el número de días entre auditorías automáticas de licencias.

AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)

Utilice este mandato para comprobar si hay incoherencias entre la información de la base de datos y un volumen de agrupación de almacenamiento. La información de proceso que se genera durante la realización de una auditoría se envía a las anotaciones de actividades y a la consola del servidor.

Restricción: No puede utilizar este mandato para volúmenes que están asignados a agrupaciones de almacenamiento de copias de contenedor.

Sólo es posible auditar volúmenes que pertenecen a agrupaciones de almacenamiento con DATAFORMAT=NATIVE y DATAFORMAT=NONBLOCK.

No se puede hacer la auditoría de un volumen si éste se está suprimiendo de una agrupación de almacenamiento primaria o de copia.

Mientras hay un proceso de auditoría activo, los clientes no pueden restaurar datos del volumen especificado ni almacenar nuevos datos en ese volumen.

Si el servidor detecta un archivo con errores, el manejo de dicho archivo dependerá del tipo de agrupación de almacenamiento al que pertenezca el volumen, de si se ha especificado la opción FIX en este mandato y de si el archivo se ha almacenado también en un volumen asignado a otras agrupaciones.

Si IBM Spectrum Protect no detecta errores para un archivo que estaba marcado como dañado, el estado del archivo se restablece para que pueda utilizarse.

El servidor no suprime las copias archivadas que están retenidas para supresión. Si la protección de retención de copias archivadas está activada, el servidor no suprimirá las copias archivadas cuyo período de retención no haya caducado.

Para visualizar información acerca del contenido de un volumen de agrupación de almacenamiento, utilice el mandato QUERY CONTENT.

Para auditar varios volúmenes, puede utilizar los parámetros FROMDATE y TODATE. Utilice el parámetro STGPOOL para auditar todos los volúmenes en una agrupación de almacenamiento. Cuando utilice los parámetros FROMDATE, TODATE o ambos, el servidor limita la auditoría sólo a los volúmenes de medios secuenciales que cumplen los criterios de fecha e incluye todos los volúmenes de disco activados del almacenamiento. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Si ejecuta un servidor con la protección de retención de archivado activada y tiene datos almacenados en agrupaciones de almacenamiento que se han definido con el parámetro RECLAMATIONTYPE=SNAPLOCK, la última fecha de acceso del archivador NetApp SnapLock para un volumen debe ser igual a la fecha de finalización del período de reclamación que ha de visualizarse al emitir un mandato QUERY VOLUME F=D en ese volumen. Durante el proceso de AUDIT VOLUME, se comparan esas fechas. Si no coinciden y el mandato AUDIT VOLUME se está ejecutando con el parámetro FIX=NO, se emitirá un mensaje indicándole que el mandato se debe ejecutar con el parámetro FIX=YES para resolver la incoherencia. Si no coinciden y el mandato AUDIT VOLUME se está ejecutando con el parámetro FIX=YES, se solucionarán las incoherencias.

Atención: Utilice el parámetro FIX=YES sólo si la unidad de cintas y la infraestructura de red de área de almacenamiento (SAN) son estables. Asegúrese de que los cabezales de cinta estén limpios y que los controladores de dispositivos estén estables y sean fiables. De lo contrario, corre el riesgo de suprimir datos sin errores cuando utilice este parámetro. El servidor no puede determinar si una cinta está dañada físicamente o si una infraestructura de cinta no es estable.

Este mandato crea un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento en la que está definido el volumen.

Sintaxis

```

                                .-Fix-----No-----
>>-AUDit Volume--+-nombre_volumen-+-----+----->
                '-| A |-----' '-Fix-----+No--+'
                                '-Yes-'

    .-SKIPPartial-----No----- .-Quiet-----No-----
>--+-----+-----+-----+-----><
    '-SKIPPartial-----+No--+' '-Quiet-----+No--+'
                '-Yes-'                '-Yes-'

A (como mínimo debe especificarse uno de estos parámetros)

|-----+----->
| (1) |
|-----STGPool-----nombreagrupación-'

    (1) (1)
    .-----FROMDate-----TODAY-. .-TODate-----TODay-----
>--+-----+-----+-----+-----|
    '-FROMDate-----date-----' '-TODate-----date-----'

```

Notas:

1. No es posible especificar un nombre de volumen si especifica un nombre de agrupación de almacenamiento, FROMDATE o TODATE.

Parámetros

nombre_volumen

Especifica el nombre del volumen de agrupación de almacenamiento que desea auditar. Este parámetro es necesario si no especifica una agrupación de almacenamiento. No es posible especificar un nombre de volumen con los parámetros FROMDATE y TODATE.

Fix

Especifica cómo el servidor resuelve las incoherencias entre el inventario de la base de datos y el volumen de agrupación de almacenamiento especificado. Este parámetro es opcional. El valor predeterminado es NO.

Las acciones que realiza el servidor dependen también de si el volumen está asignado a una agrupación de almacenamiento primaria o de copia.

Agrupación de almacenamiento primaria:

Nota: Si el mandato AUDIT VOLUME no detecta ningún error en un archivo que anteriormente se había marcado como dañado, IBM Spectrum Protect restablecerá el estado del archivo para que éste pueda utilizarse. Esto proporciona un medio de restaurar el estado de los archivos dañados si se determina que los errores son a causa de un problema de hardware corregible, como por ejemplo un cabezal de cinta que esté sucio.

Fix=No

IBM Spectrum Protect notifica, pero sin suprimirlos, los registros de la base de datos que hacen referencia a archivos con incoherencias:

- IBM Spectrum Protect marca el archivo como dañado en la base de datos. Si una copia de seguridad se almacena en una agrupación de almacenamiento de copia, el archivo puede restaurarse con el mandato RESTORE VOLUME o RESTORE STGPOOL.
- Si el archivo es una copia en caché, las referencias al archivo que haya en este volumen se pueden suprimir emitiendo el mandato AUDIT VOLUME y especificando FIX=YES. Si el archivo físico no es una copia en caché y existe un duplicado almacenado en una agrupación de almacenamiento de copia, éste puede restaurarse con el mandato RESTORE VOLUME o RESTORE STGPOOL.

Fix=Yes

El servidor arregla todas las incoherencias a medida que se detectan:

- Si el archivo es una copia en caché, el servidor suprime los registros de base de datos que hagan referencia al archivo en caché. El archivo primario se almacena en otro volumen.
- Si el archivo físico no es una copia en caché, y el archivo se almacena también en una o más agrupaciones de almacenamiento de copia, se informará acerca del error y el archivo físico se marcará como dañado en la base de datos. Puede restaurar el archivo físico con el mandato RESTORE VOLUME o RESTORE STGPOOL.
- Si el archivo físico no es una copia en caché, y el archivo físico no está almacenado en una agrupación de almacenamiento de copia, se suprimen de la base de datos todos los archivos lógicos en los que se han detectado incoherencias.
- Si la protección de retención de archivado se ha activado con el mandato SET ARCHIVERETENTIONPROTECTION, podrá suprimirse una copia en caché de los datos, si es necesario. Los datos de las agrupaciones de almacenamiento primarias y de copia sólo se pueden marcar como dañados y no se pueden suprimir nunca.

No utilice el mandato AUDIT VOLUME con FIX=YES si está ejecutándose un proceso de restauración (RESTORE STGPOOL o RESTORE VOLUME). El mandato AUDIT VOLUME podría dar lugar a que la restauración no se completara.

Agrupación de almacenamiento de copia:

Fix=No

El servidor notifica el error y marca la copia del archivo físico como dañada en la base de datos.

Fix=Yes

El servidor suprime todas las referencias al archivo físico y a los registros de la base de datos que señalen a un archivo físico que no exista.

SKIPPARTIAL

Especifica si IBM Spectrum Protect debe pasar por alto los archivos parciales, que son archivos que ocupan varios volúmenes de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Cuando se realiza una operación de auditoría en un volumen de medio de acceso secuencial, este parámetro impide montajes de medios de acceso secuencial adicionales que pueden ser necesarios para realizar una auditoría de cualquier archivo parcial. Los valores posibles son:

No

IBM Spectrum Protect audita los archivos que ocupan varios volúmenes.

A menos que especifique SKIPPARTIAL=YES, IBM Spectrum Protect intenta procesar cada archivo almacenado en el volumen, incluidos los archivos que abarcan otros volúmenes, y fuera de los mismos. Para auditar los archivos que ocupan varios volúmenes, deben cumplirse las condiciones siguientes:

- En los volúmenes de acceso secuencial, los volúmenes de acceso secuencial adicionales deben tener una modalidad de acceso de lectura/grabación o sólo lectura.
- En los volúmenes de acceso aleatorio, los volúmenes adicionales deben estar en activo.

Yes

IBM Spectrum Protect sólo audita los archivos que están almacenados en el volumen que se va a auditar. Se desconoce el estado de los archivos parciales.

Quiet

Especifica si IBM Spectrum Protect envía mensajes informativos detallados a las anotaciones de actividad y a la consola del servidor acerca de archivos irrecuperables del volumen. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que IBM Spectrum Protect envía mensajes informativos detallados y un resumen. Cada mensaje contiene el nodo, el espacio de archivos y nombre de cliente del archivo.

Yes

Especifica que IBM Spectrum Protect sólo envía un informe resumido.

FROMDate

Especifica la fecha inicial del rango para auditar volúmenes. El valor predeterminado es la fecha actual. Se auditan todos los volúmenes de medios secuenciales que cumplen los criterios de rango horario grabados con posterioridad a esta fecha. El servidor incluye todos los volúmenes de disco activados en el almacenamiento. El servidor inicia un proceso de auditoría para cada volumen y ejecuta el proceso en serie. No se puede utilizar este parámetro si se ha especificado un volumen. Este parámetro es opcional. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	10/15/2001 Si se especifica una fecha, se evaluarán todos los volúmenes candidatos que se grabaron en dicha fecha (que se inicia a las 12:00:01 am).
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para visualizar información empezando por los volúmenes grabados hace una semana, puede especificar FROMDATE=TODAY-7 o FROMDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

TODate

Especifica la fecha final del rango de volúmenes que se va a auditar. Se auditan todos los volúmenes de medios secuenciales que cumplen los criterios de rango horario grabados con anterioridad a esta fecha. El servidor incluye todos los volúmenes de disco activados en el almacenamiento. Si no especifica un valor, el servidor toma la fecha actual como valor predeterminado. No se puede utilizar este parámetro si se ha especificado un volumen. Este parámetro es opcional. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	10/15/2001 Si se especifica una fecha, se evaluarán todos los volúmenes candidatos que se grabaron en dicha fecha (que finaliza a las 11:59:59 pm).
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para visualizar la información creada hasta ayer, puede especificar TODATE=TODAY-1, o simplemente, TODATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

STGPool

Este parámetro especifica que el servidor sólo audita los volúmenes de la agrupación de almacenamiento especificada. Este parámetro es opcional. No se puede utilizar este parámetro si se ha especificado un volumen.

Ejemplo: verificar la información de base de datos de un volumen de agrupación de almacenamiento específico

Compruebe que la información de base de datos del volumen de agrupación de almacenamiento PROG2 sea coherente con los datos almacenados en el volumen. IBM Spectrum Protect arregla todas las incoherencias.

```
audit volume prog2 fix=yes
```

Ejemplo: verificar la información de base de datos de todos los volúmenes en los que se ha grabado durante un rango de fechas específico

Verifique que la información de base de datos de todos los volúmenes en los que se ha grabado entre el 20/3/2002 y el 22/3/2002 sea coherente con los datos almacenados en el volumen.

```
audit volume fromdate=03/20/2002 todate=03/22/2002
```

Ejemplo: verificar la información de base de datos de todos los volúmenes de una agrupación de almacenamiento específica

Verifique que la información de base de datos para todos los volúmenes de la agrupación de almacenamiento STPOOL3 sea coherente con los datos almacenados hoy en el volumen.

```
audit volume stgpool=STPOOL3
```

Ejemplo: verificar la información de base de datos de todos los volúmenes de una agrupación de almacenamiento específica en la que se ha grabado durante los dos últimos días

Verifique que la información de base de datos para todos los volúmenes de la agrupación de almacenamiento STPOOL3 sea coherente con los datos almacenados en el volumen durante los últimos dos días.

```
audit volume stgpool=STPOOL3 fromdate=-1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con AUDIT VOLUME

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
SET ARCHIVERETENTIONPROTECTION	Especifica si la protección de retención de datos está activada.

Mandatos BACKUP

Utilice los mandatos BACKUP para crear copias de seguridad de información u objetos IBM Spectrum Protect.

- BACKUP DB (copia de seguridad de la base de datos)
- BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)
- BACKUP NODE (Copia de seguridad de un nodo NAS)
- BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)
- BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

BACKUP DB (copia de seguridad de la base de datos)

Utilice este mandato para realizar una copia de seguridad de una base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.

Atención: Para restaurar una base de datos, el servidor debe utilizar la información del archivo de historial de volumen y el archivo de configuración de dispositivo. Debe realizar copias del archivo de historial de volumen y el archivo de configuración de dispositivo, y guardarlas. Estos archivos no pueden volver a crear.

Para determinar cuánto espacio de almacenamiento adicional necesita una copia de seguridad, emita el mandato QUERY DB.

Restricciones: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 6.3 y se está utilizando un servidor versión 7.1.

Una vez que la copia de seguridad de base de datos se ha completado, el servidor de IBM Spectrum Protect realiza una copia de seguridad de la información, en función de las opciones que se han especificado en el archivo de opciones del servidor. Se realiza una copia de seguridad de la siguiente información:

- Se realiza una copia de seguridad de la información de historial de volúmenes secuenciales en todos los archivos que la opción VOLUMEHISTORY especifica
- Se realiza una copia de seguridad de la información sobre la configuración de dispositivos en todos los archivos que la opción DEVCONFIG especifica
- La clave de cifrado maestra de servidor

Si no hay espacio suficiente en el volumen o espacio de archivos del directorio de registros activos definido, puede establecer la opción de DB2 *overflowlogpath* para utilizar un directorio que tenga el espacio disponible necesario. Por ejemplo, utilice el mandato siguiente para utilizar el directorio /home/tsminst2/overflow_dir:

```
db2 update db cfg for TSMDB1 using overflowlogpath /home/tsminst2/overflow_dir
```

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-BACKUP DB--DEVclass-----nombre_clase_dispositivo----->
. -Type-----Full-----
>+-----+----->
'-Type-----Incremental--+'
      +-Full-----+
      '-DBSnapshot--'

>+-----+----->
|               .,----- . |
|               V           | |
'-Volumenames-----+---nombre_volumen-+---+'
      '-FILE:--nombre_archivo-'

. -NUMStreams---1----- . -Scratch---Yes-----
>+-----+----->
'-NUMStreams---número-' '-Scratch---Yes--+'
      '-No--'

. -Wait---No----- . -DEDUPDevice---No-----
>+-----+----->
'-Wait---No--+' '-DEDUPDevice---No--+'
      '-Yes-'           '-Yes-'

. -COMPRESS---No----- . -PROTECTKeys---Yes-----
>+-----+----->
|               (1) | '-PROTECTKeys---No--+'
'-COMPRESS---No--+' '-Yes-'
      '-Yes-'

>+-----+----->
'-PASSWORD---nombre_contraseña-'<
```

Notas:

1. El valor predeterminado para el parámetro COMPRESS es condicional. Si especifica el parámetro COMPRESS en el mandato BACKUP DB, modifica cualquier valor de parámetro COMPRESS establecido en el mandato SET DBRECOVERY. De lo contrario, el valor establecido en el mandato SET DBRECOVERY es el valor predeterminado.

Parámetros

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial que se ha de utilizar para la copia de seguridad. Si emite el mandato BACKUP DB y la clase de dispositivo no es la especificada en el mandato SET DBRECOVERY, aparecerá un mensaje de aviso. Sin embargo, la operación de copia de seguridad continuará y no se verá afectada por ello.

Si el mandato SET DBRECOVERY no se ha emitido para definir una clase de dispositivo, el mandato BACKUP DB falla.

Restricción:

- No puede utilizar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA.
- Una operación de restauración de la base de datos falla si el origen de la restauración es una biblioteca FILE. Se crea una biblioteca FILE si la clase de dispositivo FILE especifica SHARED=YES.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la copia de seguridad, IBM Spectrum Protect cancela las operaciones con prioridad más baja como, por ejemplo, operaciones de reclamación, para que haya una unidad disponible para la copia de seguridad.

Type

Especifica el tipo de copia de seguridad que se ha de ejecutar. Este parámetro es opcional. El valor predeterminado es FULL. Son posibles los siguientes valores:

Full

Especifica que desea ejecutar una copia de seguridad completa de la base de datos de IBM Spectrum Protect.

Incremental

Especifica que desea ejecutar una copia de seguridad incremental de la base de datos de IBM Spectrum Protect. Una imagen de copia de seguridad incremental (o acumulativa) contiene una copia de todos los datos de la base de datos que se han cambiado desde la última operación satisfactoria de copia de seguridad completa.

DBSnapshot

Especifica que desea ejecutar una copia de seguridad completa de la base de datos de ADSM en un momento específico. Se copia todo el contenido de la base de datos y se crea una nueva copia de seguridad completa de la base de datos ADSM en un momento específico sin interrumpir la serie de copia de seguridad completa e incremental existente de la base de datos.

VOLUMenames

Especifica los volúmenes que se utilizan para hacer la copia de seguridad de la base de datos. Este parámetro es opcional. Sin embargo, si especifica SCRATCH=NO, debe especificar una lista de volúmenes.

nombre_volumen

Especifica los volúmenes que se utilizan para hacer la copia de seguridad de la base de datos. Puede especificar varios volúmenes separando los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre del archivo que contiene la lista de volúmenes que se utiliza para la copia de seguridad de base de datos. El nombre de cada volumen debe estar en una línea aparte. Las líneas en blanco y las líneas de comentarios, que empiezan con un asterisco, no se tienen en cuenta.

Por ejemplo, para utilizar volúmenes DB0001, DB0002 y DB0003, cree un archivo que contenga estas líneas:

```
DB0001
DB0002
DB0003
```

Asigne un nombre apropiado al archivo. Por ejemplo:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA

A continuación, puede especificar los volúmenes para el mandato, del modo siguiente:

```
 Sistemas operativos AIX  Sistemas operativos Linux
```

```
VOLUMENAMES=FILE:TAPEVOL
```

```
 Sistemas operativos Windows
```

```
VOLUMENAMES=FILE:TAPEVOL.DATA
```

NUMStreams

Especifica el número de corrientes de movimiento de datos paralelas que se utilizan cuando se realiza la copia de seguridad de la base de datos. El valor mínimo es 1 y el máximo es 32. Aumentar el valor provoca un aumento correspondiente en el número de sesiones de copia de seguridad de base de datos que se van a utilizar y en el número de unidades que se van a utilizar por clase de dispositivo. Si especifica un valor NUMSTREAMS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. De lo contrario, se utiliza el valor establecido en el mandato SET DBRECOVERY. El valor NUMSTREAMS se utiliza para todos los tipos de copias de seguridad de base de datos.

Si se especifica un valor mayor que el número de unidades disponibles para la clase de dispositivo, se utiliza el número de unidades disponibles. Las unidades disponibles son las definidas en la clase de dispositivo por el parámetro MOUNTLIMIT o por el número de unidades en línea para la clase de dispositivo especificada. La sesión se visualiza en la salida de QUERY SESSION. Si aumenta el número de corrientes, se utilizan más volúmenes de la clase de dispositivo correspondiente a esta operación. El uso de más volúmenes puede mejorar la velocidad de las copias de seguridad de base de datos, pero a expensas de que haya más volúmenes que no se utilizan completamente.

Scratch

Especifica si pueden utilizarse volúmenes reutilizables para la copia de seguridad. Este parámetro es opcional. El valor predeterminado es YES. Son posibles los siguientes valores:

Yes

Especifica que pueden utilizarse volúmenes reutilizables.

Si especifica SCRATCH=YES y el parámetro VOLUMENAMES, IBM Spectrum Protect sólo utiliza volúmenes reutilizables si no hay espacio disponible en los volúmenes especificados.

Si no incluye una lista de los volúmenes utilizando el parámetro VOLUMENAMES, debe especificar SCRATCH=YES o utilizar el valor predeterminado.

No

Especifica que no pueden utilizarse los volúmenes reutilizables.

Si especifica volúmenes con el parámetro VOLUMENAMES y SCRATCH=NO, la copia de seguridad no se hará si no hay suficiente espacio disponible para almacenar los datos de copia de seguridad en los volúmenes especificados.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. El valor predeterminado es NO. Son posibles los siguientes valores:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano BACKUP DB, puede que ya se haya realizado la copia de seguridad de parte de la base de datos antes de haberse ejecutado la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

DEDUPDevice

Especifica que el dispositivo de almacenamiento de destino da soporte a la eliminación de datos duplicados. Cuando se establece en YES, el formato de las imágenes de copia de seguridad está optimizado para los dispositivos de deduplicación de datos, lo que hace que las operaciones de copia de seguridad resulten más eficaces. Son posibles los valores siguientes:

No

Especifica que el dispositivo de almacenamiento de destino no da soporte a la eliminación de datos duplicados. NO es el valor predeterminado.

Asegúrese de que este parámetro se establece en NO para los siguientes dispositivos:

- Bibliotecas SCSI
- Todos los dispositivos definidos con una clase de dispositivo FILE
- Bibliotecas de cintas virtuales (VTL) que no soportan la función de eliminación de duplicados de datos

Yes

Especifica que un dispositivo de destino admite la eliminación de duplicados de datos y que desea optimizar las copias de seguridad para esta función. Puede establecer este parámetro en YES si está utilizando bibliotecas de cintas virtuales (VTL) que admiten la eliminación de duplicados de datos.

COMPRESS

Especifica si se comprimen los volúmenes que se crean mediante el mandato BACKUP DB. El valor COMPRESS se utiliza para todos los tipos de copias de seguridad de base de datos. Este parámetro es opcional. El valor predeterminado es conditional. Si especifica el parámetro COMPRESS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. De lo contrario, el valor establecido en el mandato SET DBRECOVERY es el valor predeterminado. Puede especificar uno de los siguientes valores:

No

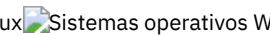
Especifica que los volúmenes que se crean mediante el mandato BACKUP DB no se comprimen.

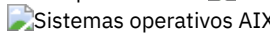
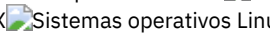
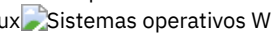
Yes

Especifica que los volúmenes que se crean mediante el mandato BACKUP DB se comprimen.

Restricciones:

- Tenga cuidado al especificar el parámetro COMPRESS. La utilización de compresión durante las copias de seguridad de la base de datos puede reducir el tamaño de los archivos de copia de seguridad. Sin embargo, la compresión puede aumentar el tiempo necesario para completar el proceso de copia de seguridad de base de datos.
- No realice copias de seguridad de datos comprimidos en una cinta. Si el entorno del sistema almacena copias de seguridad de base de datos en la cinta, establezca el parámetro COMPRESS en No en los mandatos SET DBRECOVERY y BACKUP DB.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

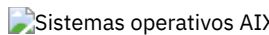
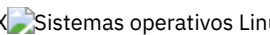
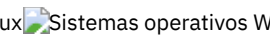
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor que se utiliza para cifrar los datos de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es el valor que se especifica para el parámetro PROTECTKEYS en el mandato SET DBRECOVERY. Puede especificar uno de los siguientes valores:

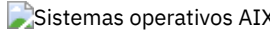
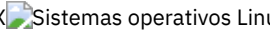
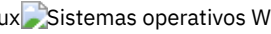
No

Especifica que las copias de seguridad de base de datos no incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=NO, debe hacer copia de seguridad de la clave de cifrado maestra manualmente para el servidor y hacer que la clave está disponible cuando implementa la recuperación tras desastre.

Yes

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Atención: Si especifica PROTECTKEYS=YES, también debe especificar el parámetro PASSWORD.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

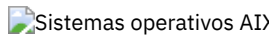
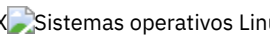
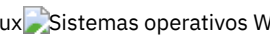
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. El valor predeterminado es el valor que se especifica para el parámetro PASSWORD en el mandato SET DBRECOVERY.

Importante: Asegúrese de que recuerda esta contraseña. Si especifica una contraseña para las copias de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos.

Ejemplo: Ejecutar una copia de seguridad incremental utilizando un volumen reutilizable

Ejecutar una copia de seguridad incremental de la base de datos, utilizando un volumen reutilizable. Utilice una clase de dispositivo FILE para la copia de seguridad.

```
backup db devclass=file type=incremental
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: Cifrar datos de agrupación de almacenamiento en copias de seguridad de base de datos

Cifrar los datos de agrupación de almacenamiento especificando que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Emita el mandato siguiente:

```
backup db protectkeys=yes password=password_name
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con BACKUP DB

Mandato	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DBRECOVERY	Especifica la clase de dispositivo que debe utilizarse para copias de seguridad automáticas.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.



BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)


Utilice este mandato para hacer copia de seguridad de la información acerca de la configuración de dispositivos del servidor.

Atención: Para restaurar una base de datos, el servidor debe utilizar la información del archivo de historial de volumen y el archivo de configuración de dispositivo. Debe realizar copias del archivo de historial de volumen y el archivo de configuración de dispositivo, y guardarlas. Estos archivos no pueden volverse a crear.

Este mandato hace copia de seguridad de la información siguiente en uno o varios archivos:

- Definiciones de clase de dispositivo
- Definiciones de biblioteca
- Definiciones de unidad
- Definiciones de ruta cuando SRCTYPE=SERVER
- Definiciones del servidor
- Nombre del servidor
- Contraseña del servidor
- Información de ubicación de volúmenes para bibliotecas LIBTYPE=SCSI

 Sistemas operativos AIX  Sistemas operativos Linux Puede utilizar la opción del servidor DEVCONFIG para especificar uno o varios archivos donde se almacenará la información de configuración de dispositivos. IBM Spectrum Protect actualiza los archivos siempre que se define, actualiza o suprime una clase de dispositivo, una biblioteca o una unidad.

 Sistemas operativos Windows En la instalación, el archivo de opciones del servidor incluye una opción DEVCONFIG que especifica un archivo de configuración de dispositivos denominado devcnfg.out. IBM Spectrum Protect actualiza este archivo siempre que se define, actualiza o suprime una clase de dispositivo, una biblioteca o una unidad.

Para garantizar que las actualizaciones se llevan cabo antes de detener el servidor:

- Después de haber emitido el mandato BACKUP DEVCONFIG, no detenga el servidor hasta que hayan transcurrido unos minutos.
- Especificar varias opciones DEVCONFIG en el archivo de opciones del servidor.
- Comprobar que se ha actualizado el archivo de configuración de dispositivos.

Clase de privilegio

Todos los administradores pueden emitir este mandato, excepto si incluye el parámetro FILENAMES. Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES, el administrador debe tener privilegio de sistema.

Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en No, el administrador debe tener privilegio de operador, de políticas, de almacenamiento o de sistema.

Sintaxis

```
>>-Backup DEVCONFig-----+-----+<<
|                               .-+-----+ |
|                               V           | |
|'-Filenames-----nombre_archivo-----+-' |
```

Parámetros

FileNames

Especifica los archivos donde debe almacenarse la información de configuración de dispositivos. Puede especificar varios archivos separándolos con comas y sin espacios intercalados. Este parámetro es opcional.

Si no especifica un nombre de archivo, IBM Spectrum Protect almacena la información en todos los archivos especificados con la opción DEVCONFIG del archivo de opciones del servidor.









Ejemplo: realizar la copia de seguridad de la información de configuración de un dispositivo en un archivo

Realizar la copia de seguridad de la información de configuración de un dispositivo en un archivo denominado DEVICE.

```
backup devconfig filenames=device
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con BACKUP DEVCONFIG

Mandato	Descripción
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux UPDATE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Cambia los atributos de una clase de dispositivo para el almacenamiento gestionado por un servidor de medios de z/OS.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

Mandato	Descripción
UPDATE PATH	Cambia los atributos asociados con una ruta.
UPDATE SERVER	Actualiza la información sobre un servidor.

BACKUP NODE (Copia de seguridad de un nodo NAS)

Utilice este mandato para iniciar una operación de copia de seguridad de un nodo de almacenamiento conectado a red (NAS).

Las copias de seguridad que se crean para nodos NAS con este mandato BACKUP NODE cuentan con funciones equivalentes a las de las copias de seguridad que se crean mediante el mandato BACKUP NAS en un cliente de IBM Spectrum Protect. Puede restaurar estas copias de seguridad con el mandato RESTORE NODE del servidor o con el mandato RESTORE NAS del cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el dominio al que está asignado el nodo o autorización de propietario de cliente en el nodo.

Sintaxis

```
>>-Backup Node--nombre_nodo----->
>+-----+----->
| .-,-----, |
| v          | |
|-----nombre_sistema_archivos---+-'
                                     .-TOC----Preferred----.
>+-----+-----+-----+----->
'-MGmtclass---clase_gest-' '-TOC---+No-----+-'
                                     +-Preferred+
                                     '-Yes-----'

.-Wait----No-----.-MODE----DIFFerential----.
>+-----+-----+-----+----->
'-Wait---+No--+-' '-MODE---+FULL-----+-'
    '-Yes-'          '-DIFFerential-'

.-TYPE----BACKUPImage----.
>+-----+-----+-----+-----><
'-TYPE---+BACKUPImage-+-'
    '-SNAPMirror--'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nodo para el que se realizará la copia de seguridad. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre_sistema_archivos

Especifica el nombre de uno o varios sistemas de archivos de los que se hará copia de seguridad. También puede especificar nombres de espacios de archivos virtuales definidos para el nodo NAS. El nombre de sistema de archivos que especifique no puede contener caracteres comodín. Puede especificar más de un sistema de archivos separando los nombres con comas y sin espacios intercalados.

Si no especifica un sistema de archivos, se hará copia de seguridad de todos los sistemas de archivos. Se realiza una copia de seguridad de todos los espacios de archivos virtuales definidos para el nodo NAS como parte de la imagen del sistema de archivos, no por separado.

Si en el dispositivo NAS existe un sistema de archivos con el mismo nombre que el espacio de archivos virtual especificado, IBM Spectrum Protect cambiará automáticamente el nombre del espacio de archivos existente en la base de datos del servidor y realizará una copia de seguridad del sistema de archivos NAS que coincide con el nombre especificado. Si el espacio de archivos virtual tiene datos de copia de seguridad, también se cambiará el nombre de la definición asociada a él.

Consejo: Consulte el parámetro del nombre del espacio de archivos virtual en el mandato DEFINE VIRTUALFSMAPPING para obtener más información acerca de las consideraciones que se aplican a la asignación de nombres.

Para determinar los sistemas de archivos que deben procesarse, el servidor no utilizará sentencias DOMAIN.NAS, INCLUDE.FS.NAS o EXCLUDE.FS.NAS en ningún archivo de opciones de cliente o conjunto de opciones de cliente. Si hace copia de seguridad de varios sistemas de archivos, cada sistema de archivos se copiará como un proceso de servidor separado.

MGmtclass

Especifica el nombre de la clase de gestión con la que se vinculan estos datos de copia de seguridad. Si no se especifica una clase de gestión, los datos de copia de seguridad se vinculan a la clase de gestión predeterminada del dominio de políticas al que está asignado el nodo. Para determinar la clase de gestión, el servidor *no* utilizará sentencias INCLUDE.FS.NAS en ningún archivo de opciones de cliente o conjunto de opciones de cliente. Puede que la clase de gestión de destino haga referencia a una agrupación nativa de IBM Spectrum Protect, en cuyo caso, los datos NDMP (Network Data Management Protocol) se enviarán a la jerarquía nativa de IBM Spectrum Protect. Después de que ello haya tenido lugar, los datos permanecerán en la jerarquía de IBM Spectrum Protect. Los datos que fluyen a las agrupaciones nativas de IBM Spectrum Protect lo hacen por medio de la LAN, y los datos que fluyen a las agrupaciones NAS pueden conectarse directamente o bien por medio de una SAN.

Cuando especifica una clase de gestión con el mandato BACKUP NODE, todas las versiones de los datos de copia de seguridad que pertenecen al nodo NAS se vuelven a vincular a la nueva clase de gestión.

TOC

Especifica si debe guardarse una tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Cuando determine si desea guardar una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se ha guardado una tabla de contenido, podrá utilizar el mandato QUERY TOC para determinar el contenido de una copia de seguridad del sistema de archivos junto con el mandato RESTORE NODE para restaurar archivos individuales o árboles de directorios. También podrá utilizar el cliente de copia de seguridad/archivado de web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y elegir los archivos y directorios que han de restaurarse. La creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Para la creación de una tabla de contenido se necesitan de forma adicional procesos, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.
- Una tabla de contenido para un sistema de archivos NAS no puede tener una ruta de directorio con más de 1024 caracteres.
- Si no se ha guardado una tabla de contenido para una copia de seguridad del sistema de archivos, todavía podrá restaurar archivos individuales o árboles de directorios utilizando el mandato RESTORE NODE siempre que conozca el nombre cualificado al completo de cada archivo o directorio que ha de restaurarse y la imagen en la que se ha realizado la copia de seguridad de ese objeto.

Este parámetro es opcional. El valor predeterminado es Preferred. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para las copias de seguridad del sistema de archivos.

Preferred

Especifica que debe guardarse la información de la tabla de contenido para las copias de seguridad del sistema de archivos. Sin embargo, la ejecución de una copia de seguridad no resultará anómala sólo porque se produzca un error durante la creación de la tabla de contenido. Éste es el valor predeterminado.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada copia de seguridad del sistema de archivos. La ejecución de una copia de seguridad resultará anómala si se produce un error durante la creación de la tabla de contenido.

Atención: Si se especifica MODE=DIFFERENTIAL y se ha solicitado una tabla de contenido (TOC=PREFERRED o TOC=YES), pero la última imagen completa no tiene ninguna, se realizará una copia de seguridad completa y se creará una tabla de contenido para esa copia de seguridad completa.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Utilice el mandato QUERY PROCESS para supervisar el proceso subordinado de este mandato.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza. Si hace copia de seguridad de varios sistemas de archivos, todos los procesos de copia de seguridad deben completarse antes de que finalice el mandato.

Atención: No se puede especificar WAIT=YES desde la consola del servidor.

MODE

Especifica si las copias de seguridad del sistema de archivos serán completas o diferenciales. El valor predeterminado es DIFFERENTIAL.

FULL

Especifica que debe hacerse copia de seguridad de todo el sistema de archivos.

DIFFerential

Especifica que sólo debe hacerse copia de seguridad de los archivos que se han modificado desde la copia de seguridad completa más reciente. Si opta por efectuar una copia de seguridad diferencial y no se encuentra una copia de seguridad completa, se realizará una copia de seguridad completa. No puede especificar TYPE=SNAPMIRROR cuando el parámetro MODE está definido como DIFFERENTIAL.

TYPE

Especifica el método de copia de seguridad utilizado para realizar la operación de copia de seguridad NDMP. El valor predeterminado para este parámetro es BACKUPIMAGE y debe utilizarse para realizar una copia de seguridad diferencial o básica estándar de NDMP. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser específicos para un servidor de archivos determinado. Los valores posibles son:

BACKUPImage

Especifica que debe hacerse una copia de seguridad del sistema de archivos utilizando una operación de vuelco NDMP. Este es el método predeterminado para realizar una copia de seguridad NDMP. La operación de tipo BACKUPIMAGE admite copias de seguridad diferenciales y completas, procesos de restauración de nivel de archivo y copias de seguridad de nivel de directorio.

SNAPMirror

Especifica que el sistema de archivos debe copiarse en una agrupación de almacenamiento de IBM Spectrum Protect utilizando la función NetApp SnapMirror to Tape. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos. Por lo general, una copia de seguridad SnapMirror se realiza en bastante menos tiempo que una copia de seguridad NDMP convencional y completa del sistema de archivos. Sin embargo, existen limitaciones y restricciones sobre el uso de las imágenes SnapMirror. La función SnapMirror to Tape está indicada para utilizarse como una opción de recuperación ante siniestro para copiar sistemas de archivos NetApp muy voluminosos en un almacenamiento secundario.

En la mayoría de los sistemas de archivos NetApp, utilice el método de copia de seguridad diferencial o completa NDMP estándar. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más información.

Cuando defina el parámetro TYPE como SNAPMirror, se aplican las siguientes restricciones:

Restricciones:

- No puede especificar TOC=YES o TOC=PREFERRED.
- El nombre_sistema_archivos no puede ser un nombre de espacio de archivos virtual.
- La instantánea que se crea automáticamente mediante el servidor de archivos durante la operación de copia de SnapMirror se suprimirá al final de la operación.
- Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM® N-Series.

Ejemplo: realizar una copia de seguridad completa

Realizar una copia de seguridad completa en el sistema de archivos /vol/vol10 del nodo NAS denominado NAS1.

```
backup node nas1 /vol/vol10 mode=full
```

Ejemplo: realizar una copia de seguridad de un directorio y crear una tabla de contenido

Realizar una copia de seguridad del directorio /vol/vol2/mikes en el nodo NAS1 y crear una tabla de contenido para la imagen. Para los dos ejemplos siguientes, se da por supuesto que la información de Tabla 1 contiene las definiciones de espacio de archivos virtual que existen en el servidor para el nodo NAS1.

```
backup node nas1 /mikesdir
```

Tabla 1. Definiciones de espacio de archivos virtual

Nombre de espacio de archivos virtual	Sistema de archivos	Ruta
/mikesdir	/vol/vol2	/mikes
/DataDirVol2	/vol/vol2	/project1/data

Nombre de espacio de archivos virtual	Sistema de archivos	Ruta
/TestDirVol1	/vol/vol1	/project1/test

Ejemplo: realizar una copia de seguridad de dos directorios

Realizar la copia de seguridad de los directorios /vol/vol2/project1/data y /vol/vol1/project1/test del nodo NAS1. Consulte la información de Tabla 1 para obtener las definiciones de espacio de archivos virtual que existen en el servidor para el nodo NAS1.

```
realizar una copia de seguridad del nodo nas1 /DataDirVol2,
/testdirvol1 mode=full toc=yes
```

Mandatos relacionados

Tabla 2. Mandatos relacionados con BACKUP NODE

Mandato	Descripción
BACKUP NAS (mandato de cliente)	Crea una copia de seguridad de datos de un nodo NAS.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
QUERY TOC	Visualiza detalles sobre la tabla de contenido para una imagen de copia de seguridad especificada.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
RESTORE NAS (mandato de cliente)	Restaura una copia de seguridad de datos de un nodo NAS.
RESTORE NODE	Restaura un nodo de almacenamiento conectado a red (NAS).
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

Conceptos relacionados:

Copia de seguridad y restauración utilizando la característica NetApp SnapMirror to Tape

BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)

Utilice este mandato para hacer copia de seguridad de los archivos de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.

Puede realizar copia de seguridad de datos desde una agrupación de almacenamiento primaria que se haya definido con el formato NATIVE, NONBLOCK, o cualquiera de los formatos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento de copia para la que va a realizarse la copia de seguridad de los datos debe tener el mismo formato de datos que la agrupación de almacenamiento primaria. IBM Spectrum Protect admite el traspaso de datos de fondo para las imágenes NDMP.

Si un archivo ya existe en la agrupación de almacenamiento de copia, no se realizará la copia de seguridad del archivo a menos que la copia del archivo que se encuentra en la agrupación de almacenamiento de copia se haya marcado como dañada. Sin embargo, no se creará una nueva copia si el archivo de la agrupación de almacenamiento primaria también se ha marcado como dañado. En una agrupación de almacenamiento de acceso aleatorio, no se hace copia de seguridad de las copias en caché de los archivos migrados ni de los archivos primarios dañados.

Consejo: La emisión de este mandato para una agrupación de almacenamiento primaria configurada para la eliminación de duplicados de datos elimina los datos duplicados, si la agrupación de almacenamiento de copia también está configurada para eliminación de duplicados de datos.

Si se inicia la migración de una agrupación de almacenamiento mientras se hace copia de seguridad de la agrupación de almacenamiento, es posible que se migren algunos archivos antes de que se haya hecho copia de seguridad de los mismos. Se

recomienda que realice una copia de seguridad de las agrupaciones de almacenamiento que estén en la parte superior de la jerarquía de migración antes de realizar la copia de seguridad de las agrupaciones de almacenamiento que se encuentren en la parte inferior.

Restricciones:

- No ejecute los mandatos MOVE DRMEDIA y BACKUP STGPOOL simultáneamente. Asegúrese de que los procesos de copia de seguridad de agrupación de almacenamiento se han completado antes de emitir el mandato MOVE DRMEDIA.
- No puede realizar la copia de seguridad de los datos desde o hasta agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento de copia en la que se han de generar las copias de seguridad.

Sintaxis

```
>>-BACkup STGpool--nom_agrupación_primaria--nom_agrupación_copia-->
. -MAXPRocess---1-----
>-----+----->
' -MAXPRocess---número-'

. -Preview ---No-----
>-----+----->
' -Preview---+No-----+
              +Yes-----+
              |           (1) |
              '-VOLumesonly-----'

. -SHREDTONoshred---No----- . -Wait---No-----
>-----+-----+-----<
' -SHREDTONoshred---+No---+ ' ' -Wait---+No---+ '
              '-Yes-'              '-Yes-'
```

Notas:

1. Sólo es válida para agrupaciones de almacenamiento que están asociadas a una clase de dispositivo de acceso secuencial.

Parámetros

agrupación_primaria (Obligatorio)

Especifica la agrupación de almacenamiento primaria.

agrupación_copia (Obligatorio)

Especifica la agrupación de almacenamiento de copia.

MAXPRocess

Especifica el número máximo de procesos paralelos a utilizar para realizar copias de seguridad de archivos. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al utilizar varios procesos paralelos, se puede mejorar el rendimiento de la copia de seguridad. Se espera que el tiempo necesario para completar la copia de seguridad de agrupación de almacenamiento disminuya al utilizar varios procesos. Sin embargo, cuando se ejecutan varios procesos, en algunos casos uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso de copia de seguridad distinto.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo secuencial no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la copia de seguridad.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia y, si el tipo de dispositivo no es FILE, también necesita una unidad. Si está haciendo copia de seguridad de una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje extra para los volúmenes de agrupación de almacenamiento primaria y, si el tipo de dispositivo no es FILE, una unidad extra. Por ejemplo, suponga que especifica un máximo de tres procesos para hacer copia de seguridad de una agrupación de almacenamiento primaria secuencial en una agrupación de almacenamiento de copia de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar

los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo seis puntos de montaje y seis unidades.

Para previsualizar una copia de seguridad, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

Preview

Especifica si se desea previsualizar la copia de seguridad sin ejecutarla. La previsualización muestra el número de archivos y bytes cuya copia de seguridad se hará y una lista de los volúmenes de agrupación de almacenamiento primaria que deberá montar. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que se hace la copia de seguridad.

Yes

Especifica que se desea previsualizar la copia de seguridad sin llevarla a cabo realmente.

VOLumesonly

Especifica que se desea previsualizar la copia de seguridad sólo como una lista de los volúmenes que deben montarse. Esta opción necesita el tiempo de proceso mínimo. La opción VOLUMESONLY sólo es válida para agrupaciones de almacenamiento asociadas a una clase de dispositivo de acceso secuencial.

La opción VOLUMESONLY puede utilizarse para obtener una lista de volúmenes que necesita el proceso de copia de seguridad de la agrupación de almacenamiento. Por ejemplo:

```
backup stgpool primary_pool copystg preview=volumesonly
```

La lista de volúmenes se registra en el registro de actividad del servidor con el mensaje ANR1228I. Realice una consulta del registro de actividad del servidor para obtener la lista de volúmenes necesarios. Por ejemplo:

```
query actlog msg=1228
```

SHREDTONOshred

Especifica si se hará una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que fuerza la destrucción. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor no permitirá que se realice una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que fuerza la destrucción. Si la agrupación de almacenamiento primaria fuerza la destrucción, la operación falla.

Yes

Especifica que el servidor sí permitirá que se realice una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que implementa la destrucción. Los datos de la agrupación de almacenamiento de copia no se destruyen cuando se eliminan.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso en segundo plano se visualizan en el registro de actividad o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si cancela este proceso, es posible que se haya hecho copia de seguridad de algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa esta operación en primer plano. Debe esperar a que la operación finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración al terminarse la operación.

Nota: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: realizar una copia de seguridad de la agrupación de almacenamiento primaria

Hacer copia de seguridad de la agrupación de almacenamiento primaria denominada PRIMARY_POOL en la agrupación de almacenamiento de copia denominada COPYSTG.

Mandatos relacionados

Tabla 1. Mandatos relacionados con BACKUP STGPOOL

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)



Utilice este mandato para hacer copia de seguridad de la información histórica de volúmenes secuenciales en uno o varios archivos.


Consejo: Debe utilizar la información histórica de volúmenes al volver a cargar la base de datos y auditar los volúmenes de agrupación de almacenamiento afectados. Si no puede iniciar el servidor, puede utilizar el archivo histórico de volúmenes para consultar la información sobre esos volúmenes en la base de datos.

El archivo histórico de volúmenes contiene información sobre los tipos de volúmenes siguientes:

- Volúmenes de anotaciones de archivado
- Volúmenes de copia de seguridad de base de datos
- Volúmenes de exportación
- Volúmenes de juegos de copias de seguridad
- Volúmenes de instantánea de base de datos
- Volúmenes de archivos del plan de recuperación de la base de datos
- Volúmenes de archivos del plan de recuperación
- Volúmenes de instantánea del archivo del plan de recuperación
- Los volúmenes de agrupación de almacenamiento de acceso secuencial siguientes:
 - Volúmenes agregados a las agrupaciones de almacenamiento
 - Volúmenes reutilizados mediante operaciones de reclamación o MOVE DATA
 - Volúmenes suprimidos con el mandato DELETE VOLUME o durante la reclamación de volúmenes reutilizables

Atención: Para restaurar una base de datos, el servidor debe utilizar la información del archivo de historial de volumen y el archivo de configuración de dispositivo. Debe realizar copias del archivo de historial de volumen y el archivo de configuración de dispositivo, y guardarlas. Estos archivos no pueden volverse a crear.

 Sistemas operativos AIX  Sistemas operativos Linux Debe utilizar la opción de servidor VOLUMEHISTORY para especificar uno o más archivos históricos de volúmenes. IBM Spectrum Protect actualiza los archivos históricos de volúmenes siempre que se cambia la información histórica de volúmenes secuenciales del servidor.

 Sistemas operativos Windows En la instalación, el archivo de opciones del servidor contiene una opción VOLUMEHISTORY que especifica un archivo histórico de volúmenes predeterminado denominado volhist.out. IBM Spectrum Protect actualiza los archivos históricos de volúmenes siempre que se cambia la información histórica de volúmenes secuenciales del servidor.

Para garantizar que las actualizaciones se llevan cabo antes de detener el servidor, siga estos pasos:

- No esperar unos minutos antes de que se detenga el servidor si se ha emitido el mandato BACKUP VOLHISTORY.

- Especificar varias opciones VOLUMEHISTORY en el archivo de opciones del servidor.
- Comprobar que se ha actualizado el archivo histórico de volúmenes.

Clase de privilegio

Todos los administradores pueden emitir este mandato, excepto si incluye el parámetro FILENAMES. Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES, el administrador debe tener privilegio de sistema. Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de políticas, de almacenamiento o de sistema.

Sintaxis

```
>>-Backup VOLHistory----->
>+-----+----->
|          .-------. |
|          v          | |
|'-Filenames-----nombre_archivo-----+'
```

Parámetros

FileNames

Especifica el nombre del archivo en el que se ha de almacenar una copia de seguridad de la información histórica de volúmenes. Puede separar varios nombres de archivo con comas y sin espacios intercalados. Este parámetro es opcional.

Si no especifica un nombre de archivo, IBM Spectrum Protect almacena la información en todos los archivos especificados con la opción VOLUMEHISTORY del archivo de opciones del servidor.

Ejemplo: realizar la copia de seguridad de la información del histórico de volúmenes en un archivo

Hacer copia de seguridad de la información histórica de volúmenes en un archivo denominado VOLHIST.

```
backup volhistory filenames=volhist
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con BACKUP VOLHISTORY

Mandato	Descripción
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

BEGIN EVENTLOGGING (Iniciar anotación de eventos)

Utilice este mandato para empezar a anotar eventos en uno o varios receptores. Un receptor para el que se ha iniciado la anotación de eventos es un *receptor activo*.

Al iniciarse el servidor, la anotación de eventos empieza automáticamente para la consola y las anotaciones de actividades, y para todos los receptores que se inician automáticamente basándose en el archivo de opciones del servidor. Puede utilizar este mandato para empezar a anotar los eventos en los receptores para los que *no* se inician automáticamente la anotación de eventos. También puede utilizar este mandato después de haber desactivado la anotación de eventos en uno o varios receptores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

```

>>-BEGIN Eventlogging----->>
| .-ALL-----|
| V |
|-----+-----+
|---+--CONSOLE-----+---+
|   +--ACTLOG-----+
|   +--EVENTSERVER----+
|   +--FILE-----+
|   +--FILETEXT-----+
|   |                   |
|   |                   | (1) |
|   +--NTEVENTLOG-----+
|   |                   |
|   |                   | (2) |
|   +--SYSLOG-----+
|   +--TIVOLI-----+
|   +--USEREXIT-----+

```

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

Parámetros

Especifique uno o varios receptores. Puede especificar varios receptores separándolos con comas sin espacios intercalados. Si especifica ALL, se inicia la anotación para todos los receptores configurados. El valor predeterminado es ALL.

ALL

Especifica todos los receptores que están configurados para la anotación de eventos.

CONSOLE

Especifica la consola del servidor como receptor.

ACTLOG

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor.

EVENTSERVER

Especifica el servidor de eventos como receptor.

FILE

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.

FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

Ejemplo: iniciar las anotaciones de eventos

Empezar a anotar eventos en las anotaciones de actividades de IBM Spectrum Protect.

```
begin eventlogging actlog
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con BEGIN EVENTLOGGING

Mandato	Descripción
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.

Mandato	Descripción
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

Mandatos CANCEL

Utilice el mandato CANCEL para finalizar una tarea o un proceso antes de que se haya completado.

- CANCEL EXPIRATION (Cancelar un proceso de caducidad)
- CANCEL EXPORT (Suprimir una operación de exportación suspendida)
- CANCEL PROCESS (Cancelar un proceso de administración)
- CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)
- CANCEL REQUEST (Cancelar una o más peticiones de montaje)
- CANCEL RESTORE (Cancelar una sesión de restauración reinicializable)
- CANCEL SESSION (Cancelar una o más sesiones cliente)

CANCEL EXPIRATION (Cancelar un proceso de caducidad)

Utilice este mandato para cancelar un número de proceso que se ejecuta como resultado de una operación de caducidad de inventario.

Utilice el mandato CANCEL EXPIRATION si no se conoce el número de proceso de caducidad; de lo contrario, utilice CANCEL PROCESS y especifique el número del proceso de caducidad. Ambos mandatos invocan el mismo código para finalizar el proceso de caducidad.

Puede utilizar el mandato CANCEL EXPIRATION para automatizar la cancelación de un proceso de caducidad. Por ejemplo, si inicia la caducidad del inventario a medianoche y, debido a la carga de trabajo de mantenimiento en el servidor, el proceso debe finalizar a las 03:00, puede planificar un mandato CANCEL EXPIRATION para que se ejecute a las 03:00 sin saber el número de proceso.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-CANcel EXPIration-----<<
```

Ejemplo: cancelar un proceso de caducidad de inventario

Cancelar el proceso que ha generado una operación de caducidad de inventario.

```
cancel expiration
```

Mandatos relacionados

Tabla 1. Mandato relacionado con CANCEL EXPIRATION

Mandato	Descripción
QUERY PROCESS	Muestra información sobre procesos subordinados.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.

CANCEL EXPORT (Suprimir una operación de exportación suspendida)

Utilice este mandato para suprimir una operación de exportación suspendida de servidor a servidor. Después de haber emitido el mandato CANCEL EXPORT, no podrá reiniciar la operación de exportación. Emita el mandato CANCEL PROCESS para suprimir una

operación de exportación que actualmente está en ejecución.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-CANcel EXPort .-*-----  
-+-----+-----><  
'---identificador_exportación---
```

Parámetros

identificador_exportación

Identificador exclusivo de la operación de exportación suspendida que desea suprimir. También puede especificar caracteres comodín en el identificador. Emita el mandato QUERY EXPORT para que se visualice una lista de las operaciones de exportación actualmente suspendidas.

Ejemplo: suprimir una operación de exportación suspendida específica

Cancelar la operación de exportación suspendida de servidor a servidor denominada EXPORTALLACCTNODES.

```
cancel export exportallacctnodes
```

Ejemplo: suprimir todas las operaciones de exportación de servidor a servidor suspendidas

Cancelar todos los procesos de exportación suspendidos de servidor a servidor.

```
cancel export *
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL EXPORT




Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

CANCEL PROCESS (Cancelar un proceso de administración)

Utilice este mandato para cancelar un proceso subordinado que haya iniciado un mandato de administración o un proceso como, por ejemplo, la migración de una agrupación de almacenamiento.

Los mandatos siguientes generan procesos subordinados:

- AUDIT CONTAINER
- AUDIT LIBRARY
- AUDIT LICENSES
- AUDIT VOLUME
- BACKUP DB
- BACKUP NODE
- BACKUP STGPOOL

- CHECKIN LIBVOLUME
- CHECKOUT LIBVOLUME
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
- CONVERT STGPOOL
- DELETE FILESPACE
- DELETE VOLUME
- EXPIRE INVENTORY
- EXPORT ADMIN
- EXPORT NODE
- EXPORT POLICY
- EXPORT SERVER
- GENERATE BACKUPSET
- IMPORT ADMIN
- IMPORT NODE
- IMPORT POLICY
- IMPORT SERVER
- MIGRATE STGPOOL
- MOVE DATA
- MOVE DRMEDIA
- MOVE MEDIA
- PREPARE
- PROTECT STGPOOL
- RECLAIM STGPOOL
- REPLICATE NODE
- RESTORE NODE
- RESTORE STGPOOL
- RESTORE VOLUME
- VARY

Las siguientes operaciones internas del servidor generan procesos subordinados:

- Caducidad de inventario
- Migración
- Reclamación

Para cancelar un proceso, debe disponer del número de proceso, que puede obtenerse mediante la emisión del mandato QUERY PROCESS.

En algunos procesos, por ejemplo la reclamación, se generan peticiones de montaje para poder finalizar el proceso. Si un proceso tiene una petición de montaje pendiente, puede que el proceso no responda a un mandato CANCEL PROCESS hasta que se haya respondido a la petición de montaje o se haya cancelado utilizando mandato REPLY o el mandato CANCEL REQUEST o bien como resultado de un tiempo de espera excedido.

Emita el mandato QUERY REQUEST para obtener una lista de las peticiones abiertas o para consultar el registro de actividad y determinar si un proceso en particular tiene pendiente una petición de montaje. Una petición de montaje indica que hace falta un volumen para el proceso actual, pero el volumen no está disponible en la biblioteca. Puede que no esté disponible el volumen si el administrador emite el mandato MOVE MEDIA o el mandato CHECKOUT LIBVOLUME o si elimina manualmente el volumen de la biblioteca.

Después de haberse emitido un mandato CANCEL PROCESS para una operación de exportación, el proceso no puede reiniciarse. Para detener una operación de exportación de servidor a servidor pero permitir que se pueda reiniciar posteriormente, emita el mandato SUSPEND EXPORT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-CANcel PProcess--número_proceso-----><
```

Parámetros

número_proceso (Obligatorio)
Especifica el número del proceso subordinado que desea cancelar.













Ejemplo: cancelar un proceso en segundo plano utilizando su número de proceso

Cancelar el proceso subordinado número 3.

```
cancel process 3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL PROCESS

Mandato	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL REQUEST	Cancela las peticiones pendientes de montaje de volúmenes.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows CONVERT STGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PROTECT STGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
REPLY	Permite que una petición siga procesándose.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)

Utilice este mandato para cancelar todos los procesos de réplica de nodos.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-CANcel REPLication-----><
```

Parámetros

Ninguno.

Ejemplo: cancelar los procesos de réplica de nodos

Cancele todos los procesos de réplica de nodo.

```
cancel replication
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL REPLICATION

Mandato	Descripción
---------	-------------

Mandato	Descripción
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.

CANCEL REQUEST (Cancelar una o más peticiones de montaje)

Utilice este mandato para cancelar una o varias peticiones de montaje de medios pendientes. Para cancelar una petición de montaje, necesita saber el número de petición asignado a la misma. Este número está incluido en el mensaje de petición de montaje y también puede mostrarse con el mandato QUERY REQUEST.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```
>>-CAnCel REQuest---número_petición+---+-----+-----><
                '-All-----'    '-PERManent-'
```

Parámetros

número_petición

Especifica el número de la petición de montaje que se ha de cancelar.

ALL

Especifica que se cancelan todas las peticiones de montaje pendientes.

PERManent

Especifica que desea que el servidor marque los volúmenes para los que está cancelando una petición de montaje como no disponibles. Este parámetro es opcional.

Ejemplo: cancelar una petición de montaje

Cancelar la petición número 2.

```
cancel request 2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL REQUEST

Mandato	Descripción
QUERY REQUEST	Muestra información acerca de todas las peticiones de montaje pendientes.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

CANCEL RESTORE (Cancelar una sesión de restauración reinicialable)

Utilice este mandato para cancelar una sesión de restauración reinicialable. Puede cancelar las sesiones de restauración que tengan el estado activo o reinicialable. Todas las peticiones de montaje pendientes relacionadas con esta sesión se cancelarán automáticamente.

Para que se visualicen las sesiones reinicialables, utilice el mandato QUERY RESTORE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de operador.

Sintaxis

```
>>-CANcel--REStore--+--número_sesión+----->>  
'-ALL-----'
```

Parámetros

número_sesión

Especifica el número de la sesión de restauración reiniciable. Una sesión activa es un número positivo y una sesión reiniciable es un número negativo.

ALL

Especifica que se han de cancelar todas las sesiones de restauración reiniciables.

Ejemplo: cancelar operaciones de restauración

Cancelar todas las operaciones de restauración.

```
cancel restore all
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL RESTORE

Mandato	Descripción
QUERY RESTORE	Muestra información acerca de las sesiones de restauración reiniciables.

CANCEL SESSION (Cancelar una o más sesiones cliente)

Utilice este mandato para cancelar sesiones existentes de nodo cliente o de administración, y para forzar la desactivación de una sesión de administración o de nodo cliente en el servidor. Todas las peticiones de montaje pendientes relacionadas con esta sesión se cancelarán automáticamente. El nodo cliente debe iniciar una nueva sesión para reanudar las actividades.

Si cancela una sesión que se encuentra en estado desocupado en espera (IdleW) la sesión de cliente volverá a conectarse automáticamente con el servidor cuando éste vuelva a iniciar el envío de datos.

Si este mandato interrumpe un proceso como, por ejemplo, de copia de seguridad o archivado, el resultado de los procesos activos en el momento de la interrupción se retrotraen y no se validan en la base de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de operador.

Sintaxis

```
>>-CANcel SEssion--+--número_sesión+----->>  
'-ALL-----'
```

Parámetros

número_sesión

Especifica el número de sesiones administrativas, de servidor o de nodo cliente que desea cancelar.

ALL

Especifica que se cancelan todas las sesiones de nodo cliente. No puede utilizar este parámetro para cancelar las sesiones de cliente o servidor administrativas.

Ejemplo: cancelar una sesión de nodo cliente específica

Cancelar la sesión de nodo cliente con NODEP (sesión 3).

```
cancel session 3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CANCEL SESSION

Mandato	Descripción
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.

CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)




Utilice este mandato para agregar un volumen de acceso secuencial o una cinta de limpieza al inventario del servidor para una biblioteca automatizada. El servidor utilizará un volumen que resida físicamente en una biblioteca automatizada hasta que dicho volumen se haya dado de alta.

Importante:

1. El proceso del mandato CHECKIN LIBVOLUME no esperará a que exista una unidad disponible, aunque la unidad sólo se encuentre en estado IDLE. Si es necesario, puede hacer que una unidad de biblioteca esté disponible emitiendo el mandato DISMOUNT VOLUME para desmontar el volumen. Después de que exista una unidad de biblioteca disponible, vuelva a emitir el mandato CHECKIN LIBVOLUME.
2. No debe definir las unidades, dar de alta medios o etiquetar los volúmenes en una biblioteca externa. El servidor proporciona una interfaz que los sistemas de gestión de medios externos utilizan para intercambiar información con el servidor.
3. Al dar de alta cintas WORM distintas de 3592, debe emplear CHECKLABEL=YES o se dan de alta como cintas de lectura/grabación normales.

Este mandato crea un proceso subordinado que puede cancelar con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis correspondiente a las bibliotecas SCSI

```
>>>CHECKIn LIBVolume--nombre_biblioteca----->
                                     .-SEARCH----No-.
>----+--nombre_volumen--+-----+-----+----->
      +-SEARCH----Yes--+-----+-----+-----+
      |                  '-| A |-'
      '-SEARCH----Bulk--+-----+-----+-----'
      |                  '-| A |-'

                                     .-OWNER----"-".
>--STATUS---+--PRivate+--+-----+-----+----->
            +-SCRatch+  '-OWNER----nombre_servidor-'
            '-CLEaner-'

                                     .-CHECKLabel---Yes----- .-SWAP---No----- .
>--+-----+-----+-----+-----+-----+----->
      '-CHECKLabel---+--Yes-----+'  '-SWAP---+--No---+'
      +-No-----+
      '-Barcode-'

                                     .-WAITTime----60----.
>--+-----+-----+-----+-----+-----+-----><
```

```
'-WAITTime----valor-' '-CLEanings-----número--'
```

```
A (SEARCH=Yes, SEARCH=Bulk)
```

```
|---+VOLRange-----nombre_volumen1,nombre_volumen2---+-----|
|           .,-----|
|           V         |
'-VOLList-----+---nombre_volumen+-----+-----|
          '-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas 349X

```
>>-CHECKIn LIBVolume--nombre_biblioteca----->
          .-SEARCH----No-.
>---+nombre_volumen---+-----+----->
  '-SEARCH----Yes-----'
        '-| A |-'
          .-OWNeR----"------
>--STATus---+---PRIVate+---+----->
  '-SCRatch-' '-OWNeR---nombre_servidor-'
          .-CHECKLabel----Yes-----
>---+-----+-----+----->
  '-CHECKLabel----+Yes+-' '-DEVType-----+3590+-'
        '-No--'           '-3592-'
          .-SWAP----No----- .-WAITTime----60----.
>---+-----+-----+----->
  '-SWAP----+No--+' '-WAITTime----valor-'
        '-Yes-'
```

```
A (SEARCH=Yes)
```

```
|---+VOLRange-----nombre_volumen1,nombre_volumen2---+-----|
|           .,-----|
|           V         |
'-VOLList-----+---nombre_volumen+-----+-----|
          '-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas ACSLS

```
>>-CHECKIn LIBVolume--nombre_biblioteca----->
          .-SEARCH----No-.
>---+nombre_volumen---+-----+----->
  '-SEARCH----Yes-----'
        '-| A |-'
          .-OWNeR----"------
>--STATus---+---PRIVate+---+----->
  '-SCRatch-' '-OWNeR---nombre_servidor-'
          .-CHECKLabel----Yes----- .-SWAP----No-----
>---+-----+-----+----->
  '-CHECKLabel----+Yes+-' '-SWAP----+No--+'
        '-No--'           '-Yes-'
          .-WAITTime----60----.
>---+-----+-----+----->
  '-WAITTime----valor-'
```

```
A (SEARCH=Yes)
```

```
|---+VOLRange-----nombre_volumen1,nombre_volumen2---+-----|
|           .,-----|
|           V         |
'-VOLList-----+---nombre_volumen+-----+-----|
          '-FILE:--nombre_archivo-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca.

nombre_volumen

Especifica el nombre de volumen del volumen de almacenamiento que se está dando de alta. Este parámetro es obligatorio si SEARCH es NO. No especifique este parámetro si SEARCH es igual a YES o BULK. Si está dando de alta un volumen en una biblioteca SCSI con varios puertos de entrada/salida, se da de alta el volumen que tenga la ranura de número más bajo.

STATus (obligatorio)

Especifica el estado del volumen. Los valores posibles son:

PRIVate

Especifica que el volumen es un volumen privado que sólo se monta si se solicita por el nombre.

SCRatch

Especifica que el volumen es un nuevo volumen reutilizable. Este volumen puede montarse para satisfacer las peticiones de montaje de volumen reutilizable durante las operaciones de almacenamiento de datos o de exportación.

Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

CLEaner

Especifica que el volumen es un cartucho limpiador y no un cartucho de datos. El parámetro CLEANINGS es necesario con los cartuchos limpiadores y debe establecerse en el número de usos del limpiador.

CHECKLABEL=YES no es válido para dar de alta un cartucho limpiador. Utilice STATUS=CLEANER para dar de alta un cartucho limpiador aparte del cartucho de datos.

OWNer

Especifica qué cliente de biblioteca es el propietario de un volumen privado en una biblioteca que se comparta en una SAN. El volumen para el que se especifique la propiedad debe ser privado. No se puede especificar una propiedad para un volumen reutilizable. Además, no se puede especificar un propietario cuando utiliza SEARCH=YES o SEARCH=BULK.

Cuando emite el mandato CHECKIN LIBVOLUME, el servidor valida el propietario. Si no especifica este parámetro, el servidor utilizará el predeterminado y delegará la propiedad del volumen al cliente de biblioteca propietario, según lo registrado en el archivo histórico de volúmenes del gestor de biblioteca. Si el volumen no es propiedad de ningún cliente de biblioteca, el servidor delegará la propiedad al gestor de biblioteca.

SEARCH

Especifica si el servidor busca en la biblioteca para localizar volúmenes que no se han dado de alta antes. Este parámetro es opcional. El valor predeterminado es NO.

Los valores posibles son:

No

Especifica que sólo se ha de dar de alta en la biblioteca el volumen indicado.

En bibliotecas SCSI: el servidor emite una solicitud para que se inserte el volumen en una ranura de cartucho en la biblioteca o, si está disponible, en un puerto de entrada. La ranura del cartucho o el puerto de entrada se identifican mediante su dirección de elemento. **En bibliotecas 349X:** el volumen puede encontrarse ya en la biblioteca o puede colocarlo en la estación de E/S cuando se le solicite.

Yes

Especifica que el servidor busca en la biblioteca los volúmenes que deben darse de alta. Se pueden utilizar los parámetros VOLRANGE o VOLLIST para limitar la búsqueda. Al utilizar este parámetro, tenga en cuenta las siguientes restricciones:

- Si la biblioteca es compartida entre aplicaciones, el servidor podría examinar un volumen requerido por otra aplicación. Para las bibliotecas 349X, el servidor solicita al gestor de bibliotecas que determine todos los volúmenes que están asignados a la categoría SCRATCH o PRIVATE, y a la categoría INSERT.
- Para las bibliotecas SCSI, no especifique a la vez SEARCH=YES y CHECKLABEL=NO en el mismo mandato.

Bulk

Especifica que el servidor busca en los puertos de Entrada/Salida de la biblioteca los volúmenes que se puedan dar de alta automáticamente. Esta opción sólo se aplica a las bibliotecas SCSI.

Importante:

1. No especifique CHECKLABEL=NO y SEARCH=BULK a la vez.
2. Puede utilizar el parámetro VOLRANGE o VOLLIST para limitar la búsqueda.

VOLRange

Especifica un rango de nombres de volúmenes, separados con comas. Puede utilizar este parámetro para limitar la búsqueda de volúmenes que deben comprobarse al especificar SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca dentro del rango especificado, el mandato finalizará sin errores.

Especifique solamente los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Los 21 se dan de alta en: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Los 3 volúmenes se dan de alta en: bar11a, bar12a, bar13a.
volrange=123400,123410	Los 11 volúmenes se dan de alta en: 123400, 123401, ...123409, 123410.

VOLLlist

Especifica una lista de volúmenes. Puede utilizar este parámetro para limitar la búsqueda de volúmenes que deben comprobarse al especificar SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca que se encuentren en la lista, el mandato finaliza sin errores.

Los valores posibles son:

nombre_volumen

Especifica uno o más nombres de valores separados por comas y sin espacios intercalados. Por ejemplo:
VOLLIST=TAPE01,TAPE02.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el mandato. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar los volúmenes TAPE01, TAPE02 y TAPE03, debe crear un archivo, TAPEVOL, que contenga las siguientes líneas:

```
TAPE01
TAPE02
TAPE03
```

Puede especificar los volúmenes para el mandato según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Atención: El nombre de archivo es sensible a las mayúsculas/minúsculas.

CHECKLabel

Especifica si el servidor debe leer etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo. Este parámetro es opcional. El valor predeterminado es YES.

Los valores posibles son:

Yes

Especifica que durante la operación de dar de alta se intenta leer la etiqueta de medio.

Atención:

1. Para las bibliotecas SCSI, no especifique a la vez SEARCH=YES y CHECKLABEL=NO en el mismo mandato.
2. Para los medios WORM distintos de 3592, debe especificar YES.

No

Especifica que durante la operación de dar de alta no se lee la etiqueta del medio. Sin embargo, si se suprime la comprobación de etiqueta pueden producirse errores en el futuro (por ejemplo, una etiqueta equivocada o un volumen etiquetado de forma incorrecta pueden ocasionar errores). En el caso de las bibliotecas 349X y ACSLS, especifique NO para evitar tener que cargar cartuchos en una unidad para leer la etiqueta del medio. Estas bibliotecas siempre devuelven la información de etiqueta externa en cartuchos y IBM Spectrum Protect utiliza esa información.

Barcode

Especifica que el servidor lee la etiqueta de código de barras si la biblioteca tiene un lector de códigos de barras y los volúmenes tienen etiquetas externas de código de barras. Puede disminuir el tiempo del proceso de dar de alta si utiliza el código de barras. Este parámetro sólo se aplica a las bibliotecas SCSI.

Si el lector de códigos de barras no puede leer una determinada etiqueta de código de barras, el servidor monta la cinta y lee la etiqueta interna.

DEVType

Especifica el tipo de dispositivo del volumen que se está dando de alta. Este parámetro es necesario si ninguna de las unidades de esta biblioteca tiene rutas definidas.

3590

Especifica que el tipo de dispositivo del volumen que se está dando de alta es 3590.

3592

Especifica que el tipo de dispositivo del volumen que se está dando de alta es 3592.

SWAP

Especifica si el servidor intercambia volúmenes, si no hay disponible una ranura de biblioteca vacía. El volumen seleccionado (el volumen de intercambio destino) para la operación de intercambio se expulsa de la biblioteca y se sustituye por el volumen que se está dando de alta. El servidor identifica un volumen de intercambio destino comprobando si hay un volumen reutilizable disponible. Si no hay ninguno, el servidor identifica el volumen montado con menor frecuencia.

Este parámetro es opcional. El valor predeterminado es NO. Este parámetro sólo tiene aplicación si se ha especificado un nombre de volumen en el mandato. Los valores posibles son:

No

Especifica que el servidor sólo da de alta el volumen si hay disponible una ranura vacía.

Yes

Especifica que si no hay disponible una ranura vacía, el servidor intercambia cartuchos para dar de alta el volumen.

WAITTime

Especifica el número de minutos que el servidor esperará su respuesta o responderá a una petición. Especifique un valor dentro del rango de 0 a 9999. Si desea que el servidor le pregunte, especifique un tiempo de espera mayor que cero. El valor predeterminado es de 60 minutos. Por ejemplo, supongamos que el servidor le solicita que inserte una cinta en el puerto de entrada/salida de una biblioteca. Si ha especificado un tiempo de espera de 60 minutos, el servidor emitirá una petición y esperará 60 minutos a que responda a la petición. Imaginemos, sin embargo, que especifica 0 como tiempo de espera. Si ya ha insertado una cinta, un tiempo de espera cero dará lugar a que la operación continúe sin que se formule ninguna pregunta. Si *no* ha insertado una cinta, un tiempo de espera igual a cero hará que la operación dé error.

CLEanings

Especifique el valor recomendado para el cartucho limpiador individual (normalmente indicado en el cartucho). El parámetro Cleanings sólo se aplica a bibliotecas SCSI. Este parámetro es necesario si STATUS=CLEANER.

Si en la biblioteca se da de alta a varios limpiadores, sólo se utilizará uno hasta que el valor CLEANINGS de éste disminuya hasta cero. A continuación, se seleccionará otro limpiador, y podrá darse de baja y descartar el primer limpiador.

Ejemplo: dar de alta a un volumen en una biblioteca SCSI

Dar de alta a un volumen denominado WPDV00 en la biblioteca SCSI denominada AUTO.

```
checkin libvolume auto wpdv00 status=scratch
```

Ejemplo: utilizar un lector de códigos de barra para explorar una biblioteca en busca de un cartucho limpiador

Explorar una biblioteca SCSI denominada AUTOLIB1 y, empleando un lector de códigos de barra, buscar el cartucho limpiador CLNV. Utilice SEARCH=YES, pero limite la búsqueda mediante el parámetro VOLLIST.

```
checkin libvolume autolib1 search=yes volland=cleanv status=cleaner  
cleanings=10 checklabel=barcode
```

Ejemplo: explorar una biblioteca para establecer los volúmenes no utilizados de un rango específico en estado de reutilización

Explorar una biblioteca 349X denominada ABC, y limitar la búsqueda al rango de volúmenes no utilizados BAR110 a BAR130, y establecer éstos en estado de reutilización.

```
checkin libvolume abc search=yes volrange=bar110,bar130  
status=scratch
```

Ejemplo: explorar una biblioteca para establecer un volumen específico en estado de reutilización

Utilizar el lector de códigos de barra para explorar una biblioteca SCSI denominada MYLIB para buscar VOL1 y establecer éste en estado de reutilización.

```
checkin libvolume mylib search=yes volland=voll status=scratch  
checklabel=barcode
```


Tabla 1. Mandatos relacionados con CHECKIN LIBVOLUME

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.




CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

Utilice este mandato para suprimir del inventario del servidor un volumen de almacenamiento de acceso secuencial de una biblioteca automatizada. Este mandato crea un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Restricciones:

1. El proceso de dar de baja no espera a que una unidad esté disponible, incluso si la unidad se encuentra en estado IDLE. Si es necesario, puede hacer que la unidad de biblioteca esté disponible desmontando el volumen con el mandato DISMOUNT VOLUME. Después de que exista una unidad disponible, podrá volver a emitir el mandato CHECKOUT LIBVOLUME.
2. Antes de dar de baja volúmenes de una biblioteca 349X, asegúrese de que el recurso de entrada y salida de cartuchos 349x disponga de suficientes ranuras vacías para dar de baja los volúmenes. El gestor de bibliotecas 3494 no informa a una aplicación de que el recurso de entrada y salida de cartuchos está lleno. Acepta peticiones de expulsión de un cartucho y espera hasta que se vacía el recurso de entrada y salida de cartuchos antes de volver al servidor. Puede parecer que IBM Spectrum Protect esté colgado, pero no lo está. Compruebe la biblioteca y borre las peticiones de intervención.
3. Antes de dar de baja volúmenes de una biblioteca ACSLS, asegúrese de que la prioridad CAP de ACSLS es mayor que cero. Si la prioridad CAP es cero, deberá especificar un valor para el parámetro CAP en el mandato CHECKOUT LIBVOLUME.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis correspondiente a las bibliotecas SCSI

```
>>-CHECKOut LIBVolume--nombre_biblioteca----->
                                     .-REMove---Bulk----.
>---+nombre_volumen+-----+----->
    '-| A |-----'   '-REMove---+Yes---+'
                               +-No---+
                               '-Bulk-'

    .-CHECKLabel---Yes----- .-FORCE---No-----
>---+-----+----->
    '-CHECKLabel---+Yes---+'   '-FORCE---+No---+'
                               '-No--'           '-Yes-'

A

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|           .-,-----|
|           V           |
'-VOLList---+---nombre_volumen+-----+'
           '-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas 349X

```
>>-CHECKOut LIBVolume--nombre_biblioteca----->
                                     .-REMove---Bulk----.
>---+nombre_volumen+-----+----->
    '-| A |-----'   '-REMove---+Yes---+'
                               +-No---+
                               '-Bulk-'

A

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|           .-,-----|
|           V           |
'-VOLList---+---nombre_volumen+-----+'
           '-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas ACSLS

```
>>-CHECKOut LIBVolume--nombre_biblioteca----->
                                     .-REMove---Yes-----
>---+nombre_volumen+-----+----->
    '-| A |-----'   '-REMove---+Yes---+'
                               +-No---+
                               '-Bulk-'

>---+-----+----->
    '-CAP---x,y,z---'

A

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|           .-,-----|
|           V           |
'-VOLList---+---nombre_volumen+-----+'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca.

nombre_volumen

Especifica el nombre del volumen.

VOLRange

Especifica dos nombres de volúmenes separados por una coma. Este parámetro es un rango de volúmenes que deben darse de baja. Si no hay volúmenes en la biblioteca dentro del rango especificado, el mandato finalizará sin errores.

Especifique solamente los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Se dan de baja los 21 volúmenes: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Se dan de baja 3 los volúmenes: bar11a, bar12a, bar13a.
volrange=123400,123410	Se dan de baja los 11 volúmenes: 123400, 123401, ...123409, 123410.

VOLLlist

Especifica una lista de los volúmenes que han de darse de baja. Si no hay volúmenes en la biblioteca que se encuentren en la lista, el mandato finaliza sin errores.

Los valores posibles son:

nombre_volumen

Especifica los nombres de uno o varios volúmenes que se utilizan para el mandato. Ejemplo: VOLLIST=TAPE01,TAPE02.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el mandato. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar los volúmenes TAPE01, TAPE02 y TAPE03, debe crear un archivo, TAPEVOL, que contenga las siguientes líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Puede especificar los volúmenes para el mandato según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Atención: El nombre de archivo es sensible a las mayúsculas/minúsculas.

REMove

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles, en función del tipo de biblioteca, son YES, BULK y NO. La respuesta del servidor a cada una de estas opciones y los valores predeterminados se describen en las siguientes secciones.

Bibliotecas 349X: El valor predeterminado es BULK. La tabla siguiente muestra cómo responde el servidor en las bibliotecas 349X.

Tabla 1. Cómo responde el servidor a bibliotecas 349X

REMOVE=YES	REMOVE=BULK	REMOVE=NO
El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.	El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.	El gestor de biblioteca 3494 no expulsa el volumen. El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

Bibliotecas SCSI: El valor predeterminado es BULK. La tabla siguiente muestra cómo responde el servidor en las bibliotecas SCSI.

Tabla 2. Cómo responde el servidor a bibliotecas SCSI

Si una biblioteca . . .	Y REMOVE=YES, ...	Y REMOVE=BULK, ...	Y REMOVE=NO, ...
No tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Posee puertos de entrada/salida y un puerto de entrada/salida <i>está disponible</i>	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Posee puertos de entrada/salida, pero <i>no hay puertos disponibles.</i>	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor espera que un puerto de entrada/salida se haga disponible.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.

Bibliotecas ACSLS: El valor predeterminado es YES. Si el parámetro se establece en YES, y el CAP tiene un valor de prioridad de selección automática de 0, se debe especificar un ID de CAP. La tabla siguiente muestra cómo responde el servidor en las bibliotecas ACSLS.

Tabla 3. Cómo responde el servidor a bibliotecas ACSLS

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho a la estación de E/S que convenga y elimina la entrada de volumen del inventario de bibliotecas del servidor.	El servidor no expulsa el cartucho. El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

CHECKLabel

Especifica si el servidor lee las etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo.

Atención: Este parámetro no sirve para las bibliotecas 349X o ACSLS de IBM®.

Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que el servidor intenta leer la etiqueta del medio para verificar que se está dando de baja el volumen correcto.

No

Especifica que durante la operación de dar de baja no se lee la etiqueta del medio. De este modo se mejora el rendimiento ya que no se produce el proceso de lectura.

FORCE

Especifica si el servidor da de baja un volumen si se produce un error de entrada/salida (E/S) al leer la etiqueta.

Atención: Este parámetro no sirve para las bibliotecas 349X o ACSLS de IBM.

Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

El servidor no da de baja un volumen de almacenamiento si se produce un error de E/S al leer la etiqueta.

Yes

El servidor da de baja el volumen de almacenamiento aunque haya un error de E/S.

CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

- x El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.
- y El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.
- z El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

Ejemplo: dar de baja un volumen y comprobar la etiqueta

Dar de baja el volumen denominado EXB004 de la biblioteca denominada FOREST. Lea la etiqueta para verificar el nombre del volumen, pero no extraiga el volumen de la biblioteca.

```
checkout libvolume forest exb004 checklabel=yes remove=no
```

Mandatos relacionados

Tabla 4. Mandatos relacionados con CHECKOUT LIBVOLUME

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

CLEAN DRIVE (Limpiar una unidad)

Utilice este mandato si desea que IBM Spectrum Protect cargue inmediatamente un cartucho limpiador en una unidad al margen de la frecuencia de limpieza.

Existen consideraciones especiales si tiene previsto utilizar este mandato con una biblioteca SCSI que proporciona limpieza automática mediante el hardware del dispositivo.

Restricción: No se puede ejecutar el mandato CLEAN DRIVE para una unidad cuyo único origen de ruta sea un servidor de archivos NAS.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-CLEAN DRIVE--nombre_biblioteca--nombre_unidad-----><
```

Parámetros

nombre_biblioteca (Necesario)
Especifica el nombre de la biblioteca a la que se asigna la unidad.

nombre_unidad (Obligatorio)
Especifica el nombre de la unidad.

Ejemplo: limpiar una unidad de cintas

Ya ha definido una biblioteca denominada AUTOLIB mediante el mandato DEFINE LIBRARY y ya ha dado de alta un cartucho limpiador en la biblioteca mediante el mandato CHECKIN LIBVOL. Informe al servidor de que la unidad TAPEDRIVE3 de esta biblioteca debe limpiarse.

```
clean drive autolib tapedrive3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con CLEAN DRIVE

Mandato	Descripción
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DRIVE	Suprime una unidad de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
UPDATE DRIVE	Cambia los atributos de una unidad.

COMMIT (controlar la validación de mandatos en una macro)

Utilice este mandato para controlar cuándo se valida un mandato en una macro y para actualizar la base de datos cuando los mandatos terminan el proceso. Si se emite en la modalidad de consola del cliente de administración, este mandato no genera ningún mensaje.

Si se produce un error durante el proceso de los mandatos de una macro, el servidor finaliza el proceso de la macro y retrotrae todos los cambios (desde la última ejecución de COMMIT). Una vez validado un mandato, no se puede suprimir por caducidad.

Si desea controlar el proceso del mandato, asegúrese de que la sesión de cliente de administración no está ejecutándose con la opción ITEMCOMMIT. La opción ITEMCOMMIT valida los mandatos de un script o de una macro a medida que se procesa *cada* mandato.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-COMMIT-----><
```

Parámetros

Ninguno.

Ejemplo: controlar la validación de los mandatos de una macro

En la modalidad interactiva del cliente de administración, registrar y otorgar autorización a los nuevos administradores utilizando una macro denominada REG.ADM. Los cambios se validarán después de que cada administrador se haya registrado y posea autorización.

Contenido de la macro:

```
/* REG.ADM-register admin políticas & otorgar autorización*/
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
COMMIT /* Validar cambios */
REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
COMMIT /* Validar cambios */
```

Mandato

```
macro reg.adm
```




Mandatos relacionados

Tabla 1. Mandatos relacionados con COMMIT

Mandato	Descripción
MACRO	Ejecuta un archivo de macro especificado.
ROLLBACK	Descarga cualquier cambio no confirmado en la base de datos desde que se ejecutó el último COMMIT.

Conceptos relacionados:

Macros de cliente administrativo

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)

Utilice este mandato para convertir una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Puede utilizar agrupaciones de almacenamiento de contenedores para la deduplicación de datos del lado de cliente y en línea.

Restricciones: Se aplican las siguientes restricciones a la conversión de la agrupación de almacenamiento:

- Sólo puede convertir una agrupación de almacenamiento una vez.
- No puede actualizar la agrupación de almacenamiento durante el proceso de la conversión. Los procesos de migración y movimiento de datos no están disponibles.
- Debe actualizar todas las políticas para garantizar que el destino especifique una agrupación de almacenamiento que no esté convertida ni en proceso de conversión.

Durante el proceso de la conversión, todos los datos de la agrupación de almacenamiento de origen se trasladan a la agrupación de almacenamiento de destino. Cuando finaliza el proceso, la agrupación de almacenamiento de origen deja de estar disponible. Cuando una agrupación de almacenamiento no está disponible, no puede grabar ningún dato en ella. La agrupación de almacenamiento de origen se puede elegir para supresión pero no se suprime automáticamente. Puede restaurar los datos a partir de la agrupación de almacenamiento de origen, si fuera necesario.

Atención: Durante la conversión de la agrupación de almacenamiento, los datos se suprimen de las agrupaciones de almacenamiento de copia y las agrupaciones de almacenamiento de datos activos. Esta acción se realiza incluso aunque haya especificado el número de días que deben transcurrir después de suprimir todos los archivos de un volumen, antes de que se pueda volver a grabar el volumen o devolver a la agrupación reutilizable.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

Sintaxis

```
>>-CONvert STGpool--source_stgpool--target_stgpool----->
```

```

.-MAXPRocess---8-----
>-----+-----+-----><
'-MAXPRocess---número---' '-DURation---minutos-'

```

Parámetros

agrupación_almacenamiento_origen (Obligatorio)

Especifique una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) para el proceso de archivado y copia de seguridad. Este parámetro es obligatorio.

agrup_alm_destino (Necesario)

Especifique el nombre de la agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube en la que se va a convertir la agrupación de almacenamiento. Este parámetro es obligatorio la primera vez que emite este mandato.

Consejo: Si reinicia la conversión de la agrupación de almacenamiento y la agrupación de almacenamiento de destino es diferente del valor que ha especificado la primera vez que ha emitido el mandato CONVERT STGPOOL, el mandato fallará.

MAXPRocess

Especifica el número máximo de procesos paralelos que se pueden utilizar para convertir datos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un número dentro del rango de 1 a 99. El valor predeterminado es 8.

Consejo: Los cambios en el valor predeterminado se guardan automáticamente. Si reinicia la conversión de la agrupación de almacenamiento y el valor de parámetro es diferente al valor especificado la primera vez que se emitió el mandato CONVERT STGPOOL, se utilizará el valor especificado más recientemente.

DURation

Especifica el número máximo de minutos que debería tardar una conversión antes de que se cancele. Cuando el número de minutos especificado transcurren, el servidor cancela todos los procesos de conversión para la agrupación de almacenamiento. Puede especificar un número dentro del rango de 1 a 9999. Este parámetro es opcional. Si no especifica este parámetro, la conversión se ejecuta hasta que se completa.

Consejo: La conversión de agrupación de almacenamiento para agrupaciones de almacenamiento grandes puede durar días. Utilice este parámetro para limitar la cantidad de tiempo de la conversión de agrupación de almacenamiento diaria. Como práctica recomendada, planifique la conversión durante al menos 2 horas para la agrupación de almacenamiento que utilice una clase de dispositivo FILE y al menos 4 horas para VTL.

Ejemplo: Convertir una agrupación de almacenamiento y especificar un número máximo de procesos

Convierta una agrupación de almacenamiento denominada DEDUPPOOL1, mueva los datos a una agrupación de almacenamiento de contenedores denominada DIRPOOL1 y especifique un máximo de 25 procesos.

```
convert stgpool deduppool1 dirpool1 maxprocess=25
```

Tabla 1. Mandatos relacionados con CONVERT STGPOOL

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.
QUERY CONVERSION	Consultar estado de conversión de una agrupación de almacenamiento.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.

Mandatos COPY

Utilice los mandatos COPY para crear una copia de los objetos o datos de IBM Spectrum Protect.

- COPY ACTIVATEDATA (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)
- COPY CLOPTSET (Copiar un conjunto de opciones de cliente)
- COPY DOMAIN (Copiar un dominio de políticas)
- COPY MGMTCLASS (Copiar una clase de gestión)

- COPY POLICYSET (Copiar un juego de políticas)
- COPY PROFILE (Copiar un perfil)
- COPY SCHEDULE (Copiar una planificación de cliente o de mandato de administración)
- COPY SCRIPT (copiar un script de IBM Spectrum Protect)
- COPY SERVERGROUP (Copiar un grupo de servidores)

COPY ACTIVEdata (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)

Utilice este mandato para copiar versiones activas de datos de copias de seguridad de una agrupación de almacenamiento primaria en una agrupación de datos activos. La principal ventaja que ofrecen las agrupaciones de datos activos son las restauraciones rápidas del cliente. Copie los datos activos regularmente para garantizar la protección de los datos ante la posibilidad de que se produzca un siniestro.

Si un archivo ya existe en la agrupación de datos activos, el archivo no se copiará a menos que la copia del archivo en la agrupación de datos activos esté marcada como dañada. Sin embargo, no se creará una nueva copia si el archivo de la agrupación de almacenamiento primaria también está marcado como dañado. En una agrupación de almacenamiento de acceso aleatorio, no se copian ni las copias en caché de los archivos migrados ni los archivos primarios dañados.

Si la migración de una agrupación de almacenamiento se inicia mientras están copiándose datos activos, puede que algunos archivos se migren antes de haberse copiado. Por este motivo, antes de copiar los datos activos de las agrupaciones de almacenamiento que ocupan una posición baja en la jerarquía de la migración, primero debe copiar los datos activos de las agrupaciones de almacenamiento que ocupan una posición más alta en la jerarquía de la migración. Antes de iniciar un proceso de copia, asegúrese de que ha completado el anterior.

Recuerde:

- Sólo puede copiar datos activos de las agrupaciones de almacenamiento que tienen un formato de datos NATIVE o NONBLOCK.
- La emisión de este mandato para una agrupación de almacenamiento primaria configurada para eliminación de duplicados elimina los datos duplicados, si la agrupación de datos activos también está configurada para eliminación de duplicados.

Clase de privilegio

Para emitir este mandato, debe disponer de privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido para la agrupación de datos activos desde la que están copiándose versiones activas de datos de copia de seguridad.

Sintaxis

```
>>-COPY ACTIVEdata--nom_agrupación_primaria--nom_agrupación_datos_act-->
. -MAXProcess---1-----
>+-----+----->
' -MAXProcess-----número--'

. -Preview ---No----- . -Wait---No-----
>+-----+----->
' -Preview---+No-----+ ' -Wait---+No---+ '
      +Yes-----+           '-Yes-'
      |                |
      |                (1) |
      +-----+
' -VOLumesonly-----'

. -SHREDTONoshred---No-----
>+-----+----->
' -SHREDTONoshred---+No---+ '
      '-Yes-'
```

Notas:

1. El parámetro VOLUMESONLY sólo se aplica a las agrupaciones de almacenamiento de acceso secuencial.

Parámetros

nombre_agrupación_primaria (Obligatorio)

Especifica la agrupación de almacenamiento primaria.

nombre_agrupación_datos_activos (Obligatorio)

Especifica la agrupación de datos activos.

MAXProcess

Especifica el número máximo de procesos paralelos que han de utilizarse para copiar archivos. Este parámetro es opcional. Especifique un valor entre 1 y 999. El valor predeterminado es 1.

Mediante la utilización de varios procesos paralelos puede mejorarse el rendimiento del mandato COPY ACTIVE DATA. Se espera que el tiempo necesario para copiar datos activos disminuirá al utilizar varios procesos. Sin embargo, cuando se ejecutan varios procesos, en algunos casos, puede que uno o varios de los procesos deban esperar para poder utilizar un volumen ya esté utilizando un proceso COPY ACTIVE DATA distinto.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, el servidor utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y de unidades disponibles depende de otras actividades de servidor y del sistema y también de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la copia de datos activos.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de datos activos y, si el tipo de dispositivo no es FILE, también necesita una unidad. Si está copiando datos activos de una agrupación de almacenamiento de acceso secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si el tipo de dispositivo no es FILE, una unidad adicional. Por ejemplo, suponga que especifica un máximo de 3 procesos para copiar una agrupación de almacenamiento primaria secuencial en una agrupación de datos activos de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de seis, y debe haber disponibles como mínimo seis puntos de montaje y seis unidades.

Para utilizar el parámetro PREVIEW, sólo se utiliza un único proceso, y no se necesitan puntos de montaje ni unidades.

Preview

Especifica si se desea previsualizar los datos activos sin copiarlos. En la previsualización se muestran el número de archivos y de bytes que han de copiarse y una lista de los volúmenes de agrupación de almacenamiento primaria que debe montar. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se copiarán los datos activos.

Yes

Especifica que se desea previsualizar el proceso pero sin copiar ningún dato.

VOLUMESONLY

Especifica que se desea previsualizar el proceso sólo como una lista de los volúmenes que deben montarse. Esta opción necesita el tiempo de proceso mínimo.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si cancela este proceso, puede que algunos archivos ya se hayan copiado antes de aplicarse la cancelación.

Yes

Especifica que el servidor realiza esta operación en primer plano. Debe esperar a que la operación finalice para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración al terminarse la operación.

No se puede especificar WAIT=YES desde la consola del servidor.

SHREDONOSHRED

Especifica si los datos deben copiarse desde una agrupación de almacenamiento primaria que aplique la destrucción a una agrupación de datos activos que no aplique la destrucción. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no permite que se copien los datos de una agrupación de almacenamiento primaria que implementa la destrucción de datos en una agrupación de datos activos que no implementa la destrucción de datos. Si la agrupación de almacenamiento primaria implementa la destrucción de datos y la agrupación de datos activos no, la operación fallará.

Yes

Especifica que el servidor permite que se copien los datos de una agrupación de almacenamiento primaria que implementa la destrucción de datos en una agrupación de datos activos que no implementa la destrucción de datos. Los datos de la agrupación de datos activos no se destruirán cuando se eliminen.

Ejemplo: copiar datos de la agrupación de almacenamiento primaria en la agrupación de datos activos

Copiar los datos activos de una agrupación de almacenamiento primaria denominada PRIMARY_POOL en una agrupación de datos activos denominada ACTIVEPOOL. Emita el mandato:

```
copy activedata primary_pool activepool
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY ACTIVEDATA

Mandato	Descripción
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

COPY CLOPTSET (Copiar un conjunto de opciones de cliente)

Utilice este mandato para copiar un conjunto de opciones de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-COpy CLOptset--nom_conjunto_opcion_actual--nuevo_nom_conjunto_opc-><
```

Parámetros

nombre_conjunto_opciones_actual (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente que se ha de copiar.

nombre_conjunto_opciones_nuevo (Obligatorio)

Especifica el nombre del nuevo conjunto de opciones del cliente. La longitud máxima del nombre es de 64 caracteres.

Ejemplo: copiar un conjunto de opciones de cliente

Copiar un conjunto de opciones de cliente denominado ENG en un nuevo conjunto de opciones denominado ENG2.

```
copy cloptset eng eng2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY CLOPTSET

Mandato	Descripción
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

COPY DOMAIN (Copiar un dominio de políticas)

Utilice este mandato para crear una copia de un dominio de políticas.

El servidor copia la información siguiente en el nuevo dominio:

- La descripción del dominio de políticas
- Los conjuntos de políticas del dominio de políticas (inclusive el conjunto de políticas ACTIVE, si se ha activado un conjunto de políticas)
- Las clases de gestión de cada juego de políticas (incluida la clase de gestión predeterminada, si se ha asignado)
- Los grupos de copia de cada clase de gestión

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-COpy DDomain--nombre_dominio_actual--nombre_nuevo_dominio----><
```

Parámetros

nombre_dominio_actual (Obligatorio)

Especifica el dominio de políticas que se copia.

nombre_nuevo_dominio (Obligatorio)

Especifica el nombre del nuevo dominio de políticas. La longitud máxima de este nombre es de 30 caracteres.

Ejemplo: copiar un dominio de políticas en un nuevo dominio de políticas

Copiar el dominio de política STANDARD a un nuevo dominio de política, ENGPOLDOM, entrando el mandato siguiente:

```
copy domain standard engpoldom
```

ENGPOLDOM ahora contiene el juego de políticas, la clase de gestión, el grupo de copia de seguridad y el grupo de copia archivada estándar.

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY DOMAIN

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

COPY MGMTCLASS (Copiar una clase de gestión)

Utilice este mandato para crear una copia de una clase de gestión en el mismo juego de políticas.

El servidor copia la información siguiente en la nueva clase de gestión:

- La descripción de la clase de gestión
- Los grupos de copia definido en la clase de gestión
- Todos los atributos de gestión de archivos para los clientes IBM Spectrum Protect for Space Management

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la nueva clase de gestión.

Sintaxis

```
>>-COpy Mgmtclass--nombre_dominio--nombre_juego_políticas----->  
>--nombre_clase_actual--nombre_nueva_clase-----><
```

Parámetros

nombre_dominio (Necesario)
Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre_juego_políticas (Necesario)
Especifica el juego de políticas al que pertenece la clase de gestión.

nombre_clase_actual (Obligatorio)
Especifica la clase de gestión que se copia.

nombre_clase_nueva (Obligatorio)
Especifica el nombre de la nueva clase de gestión. La longitud máxima de este nombre es de 30 caracteres.

Ejemplo: copiar una clase de gestión en una nueva clase de gestión

Copiar la clase de gestión ACTIVEFILES en una nueva clase de gestión denominada FILEHISTORY. La clase de gestión está en el juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS.

```
copy mgmtclass employee_records vacation  
activefiles filehistory
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY MGMTCLASS

Mandato	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

COPY POLICYSET (Copiar un juego de políticas)

Utilice este mandato para copiar un juego de políticas (inclusive el juego de políticas ACTIVE) en el mismo dominio de políticas.

El servidor copia la información siguiente en el nuevo juego de políticas:

- La descripción del juego de políticas
- Las clases de gestión de cada juego de políticas (incluida la clase de gestión predeterminada, si se ha asignado)
- Los grupos de copia de cada clase de gestión

Las políticas del nuevo conjunto de políticas no entran en vigor a menos que establezca el nuevo conjunto como conjunto de políticas ACTIVE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece el nuevo juego de políticas.

Sintaxis

```
>>-COpy Policyset--nom_dominio--nom_juego_actual--nuevo_nom_juego-><
```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el juego de políticas.

nombre_conjunto_actual (Obligatorio)

Especifica el juego de políticas que se va a copiar.

nombre_conjunto_nuevo (Obligatorio)

Especifica el nombre del nuevo juego de políticas. La longitud máxima de este nombre es de 30 caracteres.

Ejemplo: copiar un juego de políticas en un nuevo juego de políticas

Copiar el juego de políticas `VACATION` en el nuevo juego de políticas `HOLIDAY` en el dominio de políticas `EMPLOYEE_RECORDS`.

```
copy policyset employee_records vacation holiday
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

COPY PROFILE (Copiar un perfil)

Utilice este mandato en un gestor de configuración para copiar un perfil y todos los nombres de objetos asociados en un nuevo perfil.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-COpy PROFIle--nombre_perfil_actual--nombre_perfil_nuevo-----><
```

Parámetros

nombre_perfil_actual (Obligatorio)

Especifica el perfil que se copia.

nombre_perfil_nuevo (Obligatorio)

Especifica el nombre del nuevo perfil. La longitud máxima del nombre de perfil es de 30 caracteres.

Ejemplo: realizar una copia de un perfil

Copiar un perfil denominado VAL en otro perfil denominado VAL2.

```
copy profile val val2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY PROFILE

Mandato	Descripción
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

COPY SCHEDULE (Copiar una planificación de cliente o de mandato de administración)

Utilice este mandato para crear una copia de una planificación.

El mandato COPY SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones del cliente o a los mandatos de administración. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con COPY SCHEDULE

Mandato	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY SCHEDULE	Muestra información sobre planificaciones.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)
Utilice el mandato COPY SCHEDULE para crear una copia de una planificación para las operaciones de cliente. Puede copiar una planificación en un dominio de políticas o de un dominio de políticas a otro dominio de políticas. Utilice el mandato DEFINE ASSOCIATION para asociar la nueva planificación a los nodos cliente.
- COPY SCHEDULE (Crear una copia de una planificación para las operaciones de administración)
Utilice el mandato COPY SCHEDULE para crear una copia de una planificación de mandatos de administración.

COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)

Utilice el mandato COPY SCHEDULE para crear una copia de una planificación para las operaciones de cliente. Puede copiar una planificación en un dominio de políticas o de un dominio de políticas a otro dominio de políticas. Utilice el mandato DEFINE ASSOCIATION para asociar la nueva planificación a los nodos cliente.

Clase de privilegio

Para copiar una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas sin limitaciones, o privilegio de políticas limitado al dominio de políticas en el que está copiando la planificación.

Sintaxis

```
>>-COpy SChedule--nombre_dominio_actual----->
>--nombre_planificación_actual--nombre_nuevo_dominio----->
  .-nombre_planificación_actual-.  .-REPlace----No-----.
>--+-----+-----+-----+-----+-----+-----+-----><
  '-nombre_nueva_planificación--'  '-REPlace----+No--+-'
                                     '-Yes-'
```

Parámetros

nombre_dominio_actual (Obligatorio)

Especifica el nombre del dominio de políticas que contiene la planificación que desea copiar.

nombre_planif_actual (Obligatorio)

Especifica el nombre de la planificación que desea copiar.

nombre_nuevo_dominio (Obligatorio)

Especifica el nombre de un dominio de políticas en el que desea copiar la nueva planificación.

nombre_nueva_planificación

Especifica el nombre de la nueva planificación. Puede especificar hasta 30 caracteres para el nombre.

Si no especifica este nombre, se utiliza el nombre de la planificación original.

Si el nombre de la planificación ya está definido en el dominio de políticas, debe especificar REPLACE=YES o el mandato no se ejecutará.

REPlace

Especifica si se sustituye una planificación de cliente. El valor predeterminado es NO. Los valores son:

No

Especifica que la planificación de cliente no se sustituye.

Yes

Especifica que la planificación de cliente se sustituye.

Ejemplo: copiar una planificación desde un dominio de políticas hasta otro

Copiar la planificación WEEKLY_BACKUP que pertenece al dominio de políticas EMPLOYEE_RECORDS en el dominio de políticas PROG1 y denominar la nueva planificación WEEKLY_BACK2. Si ya existe una planificación definida con este nombre en el dominio de políticas PROG1, no la sustituya.

```
copy schedule employee_records weekly_backup
prog1 weekly_back2
```

COPY SCHEDULE (Crear una copia de una planificación para las operaciones de administración)

Utilice el mandato COPY SCHEDULE para crear una copia de una planificación de mandatos de administración.

Clase de privilegio

Para copiar una planificación de mandatos de administración, debe tener privilegio de sistema.

Sintaxis

```
>>-COpy SCHedule--nom_planificación_actual--nom_planificación_nuevo-->
                                     .-REPlace-----No-----
>--Type-----Administrative--+-----+-----+-----><
                                     '-REPlace-----+No--+-'
                                     '-Yes-'
```

Parámetros

nombre_planificación_actual (Obligatorio)

Especifica el nombre de la planificación que desea copiar.

nombre_planificación_nueva (Obligatorio)

Especifica el nombre de la nueva planificación. Puede especificar hasta 30 caracteres para el nombre.

Si el nombre de la planificación ya está definido, debe especificar REPLACE=YES o el mandato no se ejecutará.

Type=Administrative

Especifica que se copiará una planificación de mandato de administración.

REPlace

Especifica si se sustituye una planificación de mandato de administración. El valor predeterminado es NO. Los valores son:

No

Especifica que no se sustituye una planificación de mandato de administración.

Yes

Especifica que se sustituye una planificación de mandato de administración.

Ejemplo: copiar una planificación de mandatos de administración en otra planificación

Copiar la planificación de mandato de administración, DATA_BACKUP, y denominar la planificación DATA_ENG. Si ya existe una planificación con este nombre, se sustituirá.

```
copy schedule data_backup data_eng
type=administrative replace=yes
```

COPY SCRIPT (copiar un script de IBM Spectrum Protect)

Utilice este mandato para copiar un script de IBM Spectrum Protect existente en un nuevo script con un nombre distinto.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de operador, políticas, almacenamiento o sistema.

Sintaxis

```
>>-COpy SCRipt--nombre_script_actual--nombre_nuevo_script-----><
```

Parámetros

nombre_script_actual (Obligatorio)

Especifica el nombre del script que desea copiar.

nombre_script_nuevo (Obligatorio)

Especifica el nombre del nuevo script. Puede especificar hasta 30 caracteres para el nombre.

Ejemplo: realizar una copia de un script

Copiar el script TESTDEV en un nuevo script y denominarlo ENGDEV.

```
copy script testdev engdev
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY SCRIPT

Mandato	Descripción
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

COPY SERVERGROUP (Copiar un grupo de servidores)

Utilice este mandato para crear una copia de un grupo de servidores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-COPY SERVERGroup--nombre_grupo_actual--nombre_nuevo_grupo---><
```

Parámetros

nombre_grupo_actual (Obligatorio)

Especifica el grupo de servidores que se copia.

nombre_grupo_nuevo (Obligatorio)

Especifica el nombre del nuevo grupo de servidores. La longitud máxima de este nombre es de 64 caracteres.

Ejemplo: realizar una copia de un grupo de servidores

Copiar el grupo de servidores GRP_PAYROLL en el nuevo grupo HQ_PAYROLL.

```
copy servergroup grp_payroll hq_payroll
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con COPY SERVERGROUP

Mandato	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVER	Suprime la definición de un servidor.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVER	Actualiza la información sobre un servidor.

Mandato	Descripción
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

Utilice este mandato para especificar que los datos activos que se han copiado para un nodo de cliente de aplicaciones antes de una fecha especificada ya no son necesarios. El mandato marca los datos como inactivos para que puedan suprimirse de acuerdo con las políticas de retención de datos.

Restricción: El mandato DEACTIVATE DATA sólo es aplicable a los clientes de aplicaciones que protegen bases de datos de Oracle.

Cuando emite el mandato DEACTIVATE DATA, todos los datos de copia de seguridad activos que se almacenaron antes de la fecha especificada quedan inactivos. Los datos ya no podrán recuperarse y se suprimen cuando caducan.

El mandato DEACTIVATE DATA afecta únicamente a los archivos que se han copiado en el servidor antes de la fecha y la hora especificadas. Los archivos que se han copiado después de la fecha especificada continúan estando accesibles y el cliente todavía puede acceder al servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEACTivate DAta--nombre_nodo--TODate-----fecha----->
      .-TOTime-----23:59:59-.  .-Wait-----No-----
>-----+-----+-----+-----><
      '-TOTime-----hora-----'  '-Wait-----+No--+-'
                                      '-Yes-'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre de un nodo de cliente de aplicaciones cuyos datos se van a desactivar.

TODate (Obligatorio)

Especifica la fecha a utilizar para seleccionar los archivos de copia de seguridad que se van a desactivar. IBM Spectrum Protect desactiva únicamente los archivos cuya fecha sea la misma o anterior a la fecha que especifique. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	23/01/2014
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-30 o -30. Para desactivar los archivos con 30 días de antigüedad o más, puede especificar TODAY-30 o -30.
EOLM	Fin del último mes. El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Desactivar los archivos que estaban activos un día antes del último día del mes anterior.
BOTM	Principio de este mes. El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Desactivar los archivos que estaban activos el día 10 del mes actual.

TOTime

Especifica que desea desactivar los archivos que se han creado en el servidor antes de esta hora en la fecha especificada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Especifique la hora utilizando uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:30:22
NOW	La hora actual en la fecha especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada	NOW+03:00 o +03:00. Si emite el mandato DEACTIVATE DATA a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect desactiva los archivos que se colocaron en el servidor a las 12:00 o antes en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada	NOW-03:30 o -03:30. Si emite el mandato DEACTIVATE DATA a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect desactiva los archivos que se colocaron en el servidor a las 5:30 o antes en la fecha especificada.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Especifique los siguiente valores:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: desactivar los datos para un nodo de cliente de protección de datos

El nodo de cliente BANDIT es un cliente de aplicaciones de IBM Spectrum Protect para bases de datos: Data Protection for Oracle. Todos los datos de copia de seguridad están activos, por lo que todos los datos de copia de seguridad se retienen. El siguiente mandato desactiva los datos que se copiaron antes del 3 de enero de 2014, por lo que pueden suprimirse cuando caduquen.

```
deactivate data bandit todate=01/23/2014
```

Para desactivar los datos periódicamente para que puedan suprimirse cuando caduquen, ejecute el siguiente mandato desde una planificación de cliente.

```
deactivate data bandit todate=today
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEACTIVATE DATA

Mandato	Descripción
DECOMMISSION NODE	Pone fuera de servicio una aplicación o un sistema.
DECOMMISSION VM	Pone fuera de servicio una máquina virtual.

Mandatos DECOMMISSION

Utilice los mandatos DECOMMISSION para eliminar nodos cliente del entorno de producción. Los nodos de cliente pueden ser aplicaciones, sistemas y máquinas virtuales.

- DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)
- DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)

Utilice este mandato para eliminar del entorno de producción un nodo de cliente de una aplicación o un sistema. Cualquier copia de seguridad de los datos almacenados para el nodo de cliente caducará según la configuración de políticas a menos que suprima explícitamente los datos.

Atención: Esta acción no se puede invertir y provoca la supresión de los datos. Aunque este mandato no suprime la definición de nodo de cliente hasta que caduquen sus datos, no puede volver a poner en servicio el nodo cliente. Después de emitir este mandato, el nodo de cliente no puede acceder al servidor y no se realiza ninguna copia de seguridad de sus datos. El nodo de cliente está bloqueado y sólo puede desbloquearse para restaurar archivos. Los espacios de archivos que pertenecen al nodo de cliente, y el propio nodo de cliente, se terminan por eliminar.

Utilizando este mandato, puede poner fuera de servicio los siguientes tipos de nodos de cliente:

Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen los servidores de correo electrónico, las bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo de cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente del sistema

Los nodos de cliente del sistema incluyen las estaciones de trabajo, los servidores de archivos NAS (almacenamiento conectado a la red) y los clientes API.

Cuando un nodo de cliente ya no es necesario en el entorno de producción, puede emitir este mandato para iniciar una operación controlada y gradual para ponerlo fuera de servicio. El mandato realiza las siguientes acciones:

- Suprime todas las asociaciones de planificación del nodo de cliente. Las planificaciones ya no se ejecutan en el nodo de cliente. Esta acción es equivalente a emitir el mandato DELETE ASSOCIATION para cada planificación con la que esté asociado el nodo de cliente.
- Impide que el cliente acceda al servidor. Esta acción es equivalente a emitir el mandato LOCK NODE.

Cuando finaliza el mandato, ya no se realiza ninguna copia de seguridad de los datos del nodo de cliente en el servidor. Los datos que se han copiado antes de poner fuera de servicio el nodo de cliente no se suprimen inmediatamente del servidor. No obstante, todas las versiones de archivos de copia de seguridad, incluida la copia de seguridad más reciente, ahora son copias inactivas. Los archivos del cliente se conservan en el servidor de acuerdo con las políticas de gestión de almacenamiento.

Una vez que han caducado todos los periodos de retención de datos y se han eliminado del almacenamiento del servidor todas las copias de archivos de archivado y copia de seguridad del cliente, IBM Spectrum Protect suprime los espacios de archivos que pertenecen al nodo fuera de servicio. Esta acción es equivalente a emitir el mandato DELETE FILESPACE.

Una vez suprimidos los espacios de archivos del nodo fuera de servicio, la definición de nodo se suprime del servidor. Esta acción es equivalente a emitir el mandato REMOVE NODE.

Después de poner fuera de servicio un nodo cliente, pero antes de eliminarlo del servidor, puede utilizar el mandato QUERY NODE para comprobar que el nodo de cliente está fuera de servicio.

Restricción: No puede poner fuera de servicio un nodo de cliente que esté configurado para la réplica. Puede determinar el estado de réplica de un nodo de cliente utilizando el mandato QUERY NODE. Si un nodo de cliente está configurado para la réplica, puede eliminar el nodo de cliente de la réplica utilizando el mandato REMOVE REPLNODE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio del sistema.

Sintaxis

```
.-Wait----No-----.
```

```
>>-DECommission Node--nombre_nodo--+-----+-----><
                                     '-Wait---+No---+'
                                     '-Yes-'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo de cliente que se va a poner fuera de servicio.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: poner fuera de servicio un nodo de cliente

Ponga fuera de servicio el nodo de cliente CODY.

```
decommission node cody
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DECOMMISSION NODE

Mandato	Descripción
DECOMMISSION VM	Pone fuera de servicio una máquina virtual.
DEACTIVATE DATA	Desactiva los datos de un nodo de cliente.

DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

Utilice este mandato para eliminar una máquina virtual individual en un nodo de centro de datos. El espacio de archivos que representa la máquina virtual sólo se suprime del servidor después de que caduquen sus datos de copia de seguridad.

Atención: Este mandato no puede invertirse y provoca la supresión de los datos. Aunque este mandato no suprime el espacio de archivos de máquina virtual hasta que caduquen sus datos, no puede volver a poner en servicio la máquina virtual.

Cuando una máquina virtual ya no es necesaria en el entorno de producción, puede emitir este mandato para iniciar una eliminación por fases del espacio de archivos de máquina virtual del servidor. El mandato DECOMMISSION VM marca todos los datos que se han copiado para la máquina virtual como inactivos, para que puedan suprimirse según las políticas de retención de datos. Después de que caduquen todos los datos que se han copiado para la máquina virtual, se suprime el espacio de archivos que representa la máquina virtual. El mandato DECOMMISSION VM sólo afecta a la máquina virtual que identifique. El nodo de centro de datos y las otras máquinas virtuales que están alojadas en el nodo de centro de datos no se verán afectados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DECommission VM--nombre_nodo--nombre_vm----->
                                     .-Wait---No-----
>--+-----+-----+-----+-----><
   '-NAMEType-----FSID---' '-Wait---+Yes--'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo de centro de datos que aloja la máquina virtual que se va a poner fuera de servicio.

nombre_vm (Obligatorio)

Identifica el espacio de archivos que representa la máquina virtual que se va a poner fuera de servicio. Cada máquina virtual que está alojada en un nodo de centro de datos se representa como un espacio de archivos.

Si el nombre incluye uno o más espacios, debe escribir el nombre entre comillas dobles cuando se emita el mandato.

De forma predeterminado, el servidor interpreta el nombre del espacio de archivos que especifica utilizando la página de códigos del servidor y también intenta convertir el nombre de espacio de archivo de la página de códigos del servidor a la página de códigos UTF-8. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

Si el nombre de la máquina virtual es un nombre distinto al inglés, este parámetro debe especificar el ID del espacio de archivos (FSID). Si especifica el parámetro NAMETYPE, puede indicar al servidor que interprete el nombre de espacio de archivos por su ID de espacio de archivos (FSID) en su lugar.

NAMETYPE

Especifique cómo desea que el servidor interprete el nombre de espacio de archivos especificado para identificar la máquina virtual. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede especificar el siguiente valor:

FSID

El servidor interpreta el nombre de espacio de archivos por su identificador de espacio de archivos (FSID).

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplos: Dejar fuera de servicio una máquina virtual

Ponga fuera de servicio la máquina virtual CODY.

```
decommission vm dept06node cody
```

Dejar fuera de servicio la máquina virtual

```
decommission vm dept06node "cody 2"
```

Ponga fuera de servicio una máquina virtual especificando su ID de espacio de archivos.

```
decommission vm dept06node 7 nametype=fsid
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DECOMMISSION VM

Mandato	Descripción
DECOMMISSION NODE	Pone fuera de servicio una aplicación o un sistema.
DEACTIVATE DATA	Desactiva los datos de un nodo de cliente.

Mandatos DEFINE

Utilice los mandatos DEFINE para crear objetos de IBM Spectrum Protect.

- DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)
- DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)
- DEFINE BACKUPSET (Definir un juego de copias de seguridad)
- DEFINE CLIENTACTION (Definir una acción de cliente única)
- DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)
- DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)
- DEFINE COLLOGROUP (Definir un grupo de proximidad)
- DEFINE COLLOCMEMBER (Definir un miembro de grupo de proximidad)
- DEFINE COPYGROUP (Definir un grupo de copia)
- DEFINE DATAMOVER (Definir un transportador de datos)
- DEFINE DEVCLASS (Definir una clase de dispositivo)
- DEFINE DOMAIN (Definir un nuevo dominio de políticas)
- DEFINE DRIVE (Definir una unidad en una biblioteca)
- DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)
- DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)
- DEFINE LIBRARY (Definir una biblioteca)
- DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)
- DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)
- DEFINE MGMTCLASS (Definir una clase de gestión)
- DEFINE NODEGROUP (Definir un grupo de nodos)
- DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)
- DEFINE PATH (Definir una ruta)
- DEFINE POLICYSET (Definir un juego de políticas)
- DEFINE PROFASSOCIATION (Definir una asociación de perfil)
- DEFINE PROFILE (Definir un perfil)
- DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)
- DEFINE RECOVERYMEDIA (Definir medio de recuperación)
- DEFINE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)
- DEFINE SCRIPT (definir un script de IBM Spectrum Protect)
- DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)
- DEFINE SERVERGROUP (Definir un grupo de nodo)
- DEFINE SPACETRIGGER (Definir desencadenante de espacio)
- DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)
- DEFINE STGRULE (Definir una regla de almacenamiento para agrupaciones de almacenamiento)
- DEFINE STGPOOL (Definir una agrupación de almacenamiento)
- DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)
- DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)
- DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)
- DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)

DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)

Utilice este mandato para desencadenar una alerta siempre que un servidor emita un determinado mensaje de error. Puede definir un número de mensaje para que sea un desencadenante de alerta, asignarlo a una categoría o especificar administradores a los que se pueda notificar de la alerta por correo electrónico.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
          .-n-----  
          v         |  
>>-Define ALERTTrigger-----+---número_mensaje-+----->  
  
          .-CATegory----Server-----  
>--+-----+----->  
          '-CATegory----+Application-+-'  
                +-INventory---+  
                +-CLient-----+
```

```

+-DEvice-----+
+-SErver-----+
+-STorage-----+
+-SYstem-----+
'-VMclient-----'

>-----<
|          .-,'-----'          |
|          v                      |
|'-ADmin-----nombre_admin-+'|

```

Parámetros

número_mensaje (Obligatorio)

Especifica el número de mensaje que desea asociar con el desencadenante de la alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres.

CATegory

Especifica el tipo de categoría de la alerta, que está determinado por los tipos de mensajes. El valor predeterminado es SERVER.

Nota: Si se cambia la categoría de un desencadenante de alerta, no se cambia la categoría de las alertas existentes en el servidor. Las nuevas alertas se clasifican dentro de la nueva categoría.

Especifique uno de los siguientes valores:

APplication

La alerta se clasifica como una categoría de aplicación. Por ejemplo, puede especificar esta categoría para los mensajes asociados con los clientes de aplicación (TDP).

INventory

La alerta se clasifica como categoría de inventario. Por ejemplo, puede especificar esta categoría para mensajes que están asociados con la base de datos, el archivo de registro activo o el archivo de registro de archivado.

CLient

La alerta se clasifica como una categoría de cliente. Por ejemplo, puede especificar esta categoría para los mensajes asociados con actividades de cliente generales.

DEvice

La alerta se clasifica como una categoría de dispositivo. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados a las clases de dispositivos, bibliotecas, unidades o vías de acceso.

SErver

La alerta se clasifica como una categoría de servidor general. Por ejemplo, puede especificar esta categoría para los mensajes asociados a las actividades del servidor generales o a sucesos.

STorage

La alerta se clasifica como una categoría de almacenamiento. Por ejemplo, puede especificar esta categoría para los mensajes asociados con las agrupaciones de almacenamiento.

SYstems

La alerta se clasifica como una categoría de clientes del sistema. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con los clientes de archivado y copia de seguridad del sistema o archivado y copia de seguridad de gestión de almacenamiento jerárquico (HSM).

VMclient

La alerta se clasifica bajo la categoría VMclient. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con clientes de máquina virtual.

ADmin

Este parámetro opcional especifica el nombre del administrador que recibe el correo electrónico de notificación de esta alerta. El desencadenante de alerta se ha definido satisfactoriamente aunque no se ha especificado ningún nombre de administrador.

Asignar dos números de mensaje a una alerta

Emita el siguiente mandato para especificar que desea que dos números de mensaje desencadenen una alerta:

```
define alertrigger ANR1067E,ANR1073E
```

Asignar un número de mensaje a una alerta y enviarlo por correo electrónico a dos administradores

Emita el mandato siguiente para especificar los números de mensaje que desea que desencadenen una alerta y hacer que se envíen por correo electrónico a dos administradores:

```
define alertrigger ANR1067E,ANR1073E ADmin=BILL,DJADMIN
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE ALERTRIGGER

Mandato	Descripción
DELETE ALERTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)

Utilice este mandato para asociar uno o varios clientes a una planificación. Debe asignar un nodo de cliente al dominio de políticas al que pertenezca la planificación. Los nodos cliente procesan las operaciones según las planificaciones asociadas a los nodos.

Nota:

1. IBM Spectrum Protect no puede ejecutar varias planificaciones al mismo tiempo para el mismo nodo de cliente.
2. En una macro, es posible que el servidor se detenga si algunos mandatos (por ejemplo, REGISTER NODE y DEFINE ASSOCIATION) no se han validado inmediatamente después de haberlos emitido. Puede especificar que todos los mandatos de una macro vayan seguidos de COMMIT. Sin embargo, una solución más sencilla consiste en incluir la opción ITEMCOMMIT en el mandato DSMADMC.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio de políticas al que pertenece la planificación

Sintaxis

```
>>-DEFine ASSOCIation--nombre_dominio--nombre_planificación----->
      .-,------.
      v           |
>----nombre_nodo+-----><
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación que desea asociar con uno o más clientes.

nombre_nodo (Obligatorio)

Especifica el nombre de un nodo de cliente o una lista de nodos cliente que se ha de asociar a la planificación especificada. Debe separar los elementos de la lista con comas. No deje espacios en blanco entre los elementos y las comas. Puede utilizar un carácter comodín para especificar un nombre. El mandato no asociará un cliente de la lista con la planificación si:

- El cliente ya está asociado con la planificación especificada.
- El cliente no está asignado al dominio de políticas al que pertenece la planificación.
- El cliente es un nombre de nodo NAS. Todos los nodos NAS se pasarán por alto.

Ejemplo: asociar nodos cliente a una planificación

Asociar los nodos cliente SMITH o JOHN a la planificación WEEKLY_BACKUP. Los clientes asociados están asignados al dominio de políticas EMPLOYEE_RECORDS.

```
define association employee_records
weekly_backup smith*,john*
```

Ejemplo: asociar nodos cliente a una planificación

Asociar los nodos cliente JOE, TOM y LARRY a la planificación WINTER. Los clientes asociados están asignados al dominio de políticas EMPLOYEE_RECORDS; sin embargo, el cliente JOE ya está asociado con la planificación WINTER.

```
define association employee_records
winter joe,tom,larry
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE ASSOCIATION

Mandato	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
DELETE ASSOCIATION	Suprime la asociación entre los clientes y una planificación.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.

DEFINE BACKUPSET (Definir un juego de copias de seguridad)

Utilice este mandato para definir un conjunto de copias de seguridad de cliente que anteriormente se había generado en un servidor y ponerlo a disposición del servidor que está ejecutando este mandato. El nodo cliente tiene la opción de restaurar el conjunto de copias de seguridad desde el servidor que ejecuta este mandato en lugar de hacerlo en el que se generó el conjunto de copias de seguridad.

Cualquier conjunto de copias de seguridad que se haya generado en un servidor puede definirse para otro servidor cuando los servidores comparten un tipo de dispositivo común. El nivel del servidor para el que se está definiendo el conjunto de copias de seguridad debe ser igual o más alto que el nivel del servidor que ha generado el conjunto de copias de seguridad.

También puede utilizar el mandato DEFINE BACKUPSET para volver a definir un juego de copias de seguridad que se había suprimido en un servidor.

Clase de privilegio

Si la opción del servidor REQSYSAUTHOUTFILE se establece en YES (el valor predeterminado), el administrador deberá disponer de privilegio de sistema. Si la opción del servidor REQSYSAUTHOUTFILE se establece en NO, el administrador deberá disponer de privilegio de sistema o de privilegio de políticas para el dominio al que se ha asignado el nodo cliente.

Sintaxis

```
      .-,-----
      v          |
>>-DEFine BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'

>>--prefijo_nombre_juego_copias_seguridad----->

>>--DEVclass-----nombre_clase_dispositivo----->

      .-,-----
      v          |
>>--VOLumes-----nombres_volúmenes----->

      .-RETention-----365-----.
```

```

>-----+-----+-----+-----+-----+----->
'-REtention--++-+días---+-'
          '-NOLimit-'

>-----+-----+-----+-----+-----+----->
'-DEScRiption----descripción-'

.-WHEREDATAType----ALL-----
>-----+-----+-----+-----+-----+----->
|           .-,-----|
|           v           |
'-WHEREDATAType-----+FILE--+--+'
          '-IMAGE-'

>-----+-----+-----+-----+-----+----->
'-TOC----++-+PREFERRED+-'
          +-YES-----+
          '-NO-----'

>-----+-----+-----+-----+-----+-----<
'-TOCMGmtclass----nombre_clase-'

```

Parámetros

nombre_nodo o nombre_grupo_nodos (Necesario)

Especifica el nombre de los nodos cliente o grupos de nodos cuyos datos se incluyen en los volúmenes de juegos de copias de seguridad especificados. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Si los volúmenes de conjuntos de copias de seguridad contienen conjuntos de copias de seguridad de varios nodos, se define cada conjunto de copias de seguridad cuyo nombre de nodo coincide con uno de los nombres de nodo especificados. Si los volúmenes contienen un conjunto de copias de seguridad para un nodo que actualmente no está registrado, el mandato DEFINE BACKUPSET no define el conjunto de copias de seguridad para dicho nodo.

prefijo_nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a definir en este servidor. La longitud máxima del nombre es de 30 caracteres.

Cuando se selecciona un nombre, IBM Spectrum Protect agrega un sufijo para crear el nombre de juego de copias de seguridad. Por ejemplo, si especifica el nombre del juego de copias de seguridad *mybackupset*, IBM Spectrum Protect agrega un número exclusivo como, por ejemplo, 3099, al nombre. El nombre de juego de copias de seguridad se identifica como *mybackupset.3099*. Si más adelante desea ver información acerca de este juego de copias de seguridad, puede especificar un carácter comodín en el nombre, como por ejemplo, *mybackupset** o puede especificar el nombre completo como *mybackupset.3099*.

Si los volúmenes de conjuntos de copias de seguridad contienen conjuntos de copias de seguridad para varios nodos, los conjuntos de copias de seguridad se definen para cada nodo utilizando el mismo prefijo y sufijo del nombre del conjunto de copias de seguridad.

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo de los volúmenes para los que se lee el juego de copias de seguridad.

Nota: El tipo de dispositivo que está asociado con la clase de dispositivo que especifique debe coincidir con la clase de dispositivo con la que el conjunto de copias de seguridad se generó originalmente.

VOLumes (Obligatorio)

Especifica los nombres de los volúmenes que se utilizan para almacenar el conjunto de copias de seguridad. Puede especificar varios volúmenes separando los nombres con comas y sin espacios intercalados. Los volúmenes que especifique deben estar disponibles en el servidor que está definiendo el conjunto de copias de seguridad.

Nota: Los volúmenes que especifique deben estar en el orden en el que se crearon o el mandato DEFINE BACKUPSET no se ejecutará correctamente.

El servidor no verifica si cada volumen especificado para un conjunto de copias de seguridad de varios volúmenes contiene parte del conjunto de copias de seguridad. El primer volumen siempre se comprueba y en algunos casos también se comprueban otros volúmenes adicionales. Si estos volúmenes son correctos, se define el conjunto de copias de seguridad y todos los volúmenes que figuran en la lista del mandato quedan protegidos frente a la sobregrabación. Si un volumen que contiene parte del conjunto de copias de seguridad no figura en la lista del mandato, el volumen no queda protegido y puede sobregrabarse potencialmente durante las operaciones normales del servidor.

Nota: El servidor intenta, de manera predeterminada, crear una tabla de contenido cuando se define un conjunto de copias de seguridad. Si se especifica un volumen incorrecto, o si los volúmenes no figuran en la lista en el orden correcto, la creación de la tabla de contenido falla. Si se produce este error, compruebe la lista de volúmenes del mandato y opte por utilizar el mandato QUERY BACKUPSETCONTENTS para verificar el contenido del conjunto de copias de seguridad.

RETention

Especifica el número de días que se retiene en el servidor el juego de copias de seguridad. Puede especificar un entero de 0 a 30000. El valor predeterminado es 365 días. Los valores son:

días

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor.

NOLimit

Especifica que el conjunto de copias de seguridad debe retenerse indefinidamente en el servidor.

Si especifica NOLIMIT, IBM Spectrum Protect retiene los volúmenes que contienen el conjunto de copias de seguridad sin límite de tiempo, a menos que un usuario o un administrador suprima los volúmenes del almacenamiento del servidor.

DESCRiption

Especifica la descripción que se asociará al juego de copias de seguridad que pertenece al nodo cliente. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

WHEREDATAType

Especifica que se van a definir los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben definir. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben definir. ALL es el valor predeterminado.

FILE

Especifica que se va a definir un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad.

IMAGE

Especifica que se va a definir un juego de copias de seguridad de imagen. Los conjuntos de copias de seguridad de imagen contienen imágenes que ha creado el mandato BACKUP IMAGE del cliente de archivado y copia de seguridad.

TOC

Especifica si debe crearse una tabla de contenido (TOC) para el conjunto de copias de seguridad de nivel de archivo cuando éste se defina. Cuando defina conjuntos de copias de seguridad de datos de aplicación y de imagen se ignorará el parámetro TOC porque siempre se crea una tabla de contenido para estos conjuntos de copias de seguridad.

Cuando determine si desea crear una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se crea una tabla de contenido, podrá utilizar el cliente de archivado de copia de seguridad web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y elegir los archivos y directorios que han de restaurarse. Para crear una tabla de contenido debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión que ha especificado el parámetro TOCMGMTCLASS. Para crear una tabla de contenido, se necesitan de forma adicional procesos, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación del conjunto de copias de seguridad.
- Si no se guarda una tabla de contenido para un conjunto de copias de seguridad, todavía puede restaurar archivos individuales o árboles de directorios mediante el mandato RESTORE BACKUPSET del cliente de archivado y copia de seguridad, siempre que conozca el nombre completo de cada archivo o directorio que se desea restaurar.

Este parámetro es opcional. El valor predeterminado es Preferred. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para los juegos de copias de seguridad de nivel de archivo.

Preferred

Especifica que debe guardarse la información de la tabla de contenido para conjuntos de copias de seguridad de nivel de archivo. Sin embargo, un juego de copias de seguridad no fallará sólo porque se produzca un error durante la creación de la tabla de contenido.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada juego de copias de seguridad de nivel de archivo. Un juego de copias de seguridad fallará si se produce un error durante la creación de la tabla de contenido.

TOCMGmtclass

Especifica el nombre de la clase de gestión a la que la tabla de contenido debe estar vinculada. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado

el nodo. En este caso, la creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

Ejemplo: definir un juego de copias de seguridad

Defina el conjunto de copias de seguridad PERS_DATA que pertenece al nodo cliente JANE en el servidor que está ejecutando este mandato. Retener el juego de copias de seguridad en el servidor durante 50 días. Especifique que los volúmenes VOL001 y VOL002 contienen los datos del juego de copias de seguridad. Los volúmenes los ha de leer un dispositivo asignado a la clase de dispositivo AGADM. Incluya una descripción.

```
define backupset jane pers_data devclass=agadm
volumes=vol1,vol2 retention=50
description="sector 7 base image"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE BACKUPSET

Mandato	Descripción
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

DEFINE CLIENTACTION (Definir una acción de cliente única)

Utilice este mandato para planificar uno o varios clientes para que procesen un mandato de una acción única.

El servidor define automáticamente una planificación y asocia el nodo cliente a la planificación. El servidor asigna la prioridad de planificación 1, establece PERUNITS en ONETIME y determina el número de días que se debe mantener activa la planificación. El número de días se basa en el valor que se ha establecido con el mandato SET CLIENTACTDURATION.

La rapidez con que el cliente procesa este mandato depende de si la modalidad de planificación del cliente está definida en "por petición de servidor" o "por sondeo de cliente". El planificador del cliente debe estar iniciado en la estación de trabajo cliente para que el servidor pueda procesar la planificación.

Recuerde: El inicio del planificador de IBM Spectrum Protect depende del proceso de las otras hebras del servidor y de otros procesos del sistema principal del servidor de IBM Spectrum Protect. El plazo de tiempo necesario para iniciar el planificador también depende del tráfico de la red y del tiempo que se necesita para abrir un socket, para establecer la conexión con el cliente de IBM Spectrum Protect y para recibir una respuesta del cliente. En general, cuanto más numerosos sean los requisitos de proceso y de conectividad del cliente y del servidor de IBM Spectrum Protect, más tiempo tardará en iniciarse el planificador.

Clase de privilegio

Para emitir este mandato debe tener privilegio de sistema y privilegio de política o bien sin restricciones, o bien restringido al dominio de políticas al que pertenece la planificación.

Sintaxis

Cuando especifique ACTION=RESTORE para una operación planificada y se define la opción REPLACE como PROMPT, no se efectúa ninguna petición. Si establece la opción en PROMPT, se ignoran los archivos.

Si se especifica una segunda especificación de archivo, ésta actúa como destino de la restauración. Si necesita restaurar varios grupos de archivos, planifique una restauración para cada especificación de archivo que necesita restaurar.

RETRieve

Indica que la planificación recupera los archivos especificados con el parámetro OBJECTS.

Recuerde: Un segundo archivo especificado actúa como el destino de recuperación. Si necesita recuperar varios grupos de archivos, cree una planificación distinta para cada grupo de archivos.

IMAGEBACKup

Especifica que la planificación hace copia de seguridad de los volúmenes lógicos especificados con el parámetro OBJECTS.

IMAGERESStore

Especifica que la planificación restaura los volúmenes lógicos especificados con el parámetro OBJECTS.

Mandato

Indica que la planificación procesa un mandato de un sistema operativo de cliente o un script, especificado con el parámetro OBJECTS.

Macro

Especifica que un cliente procesa una macro cuyo nombre de archivo se especifica con el parámetro OBJECTS.

SUBACTion

Puede especificar uno de los siguientes valores:

""

Cuando una serie vacía (dos dobles comillas) se especifica con ACTION=BACKUP, la copia de seguridad es incremental.

FASTBacK

Especifica que una operación de cliente FastBack identificada por el parámetro ACTION se va a planificar para procesar. El parámetro ACTION debe ser ARCHIVE o BACKUP.

SYSTEMState

Especifica que se ha programado una copia de seguridad del estado del sistema.

VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

VM


Especifica que se ha programado una copia de seguridad VMware del cliente.

OPTions

Especifica las opciones que se especifican en el mandato planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el mandato planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de mandatos. Todas las opciones que se describen como válidas solamente en la línea de mandatos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el mandato planificado:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el mandato DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el mandato planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:
 - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Para especificar `domain all-local -c: -d:`, escriba:
 - `options='-domain="all-local -c: -d:"'`

Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

OBJECTS

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando `ACTION=INCREMENTAL`. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un mandato o una macro, el objeto será el nombre del mandato o macro que debe ejecutarse.

Si especifica `ACTION=INCREMENTAL` sin especificar ningún valor para este parámetro, el mandato planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de
destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número
excesivo de argumentos de línea de
mandatos
```

Si especifica `ACTION=ARCHIVE`, `INCREMENTAL` o `SELECTIVE` para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.

Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofos. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofos. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar `C:\ARCHIVO 2`, `D:\ARCHIVOS GIF` y `E:\ARCHIVO DE PRUEBA`, escriba:
 - `OBJECTS=' "C:\ARCHIVO 2" "D:\ARCHIVOS GIF" "E:\ARCHIVO DE PRUEBA" '`
- Para especificar `D:\ARCHIVO DE PRUEBA`, escriba:
 - `OBJECTS=' "D:\ARCHIVO DE PRUEBA" '`
- Para especificar `D:\PRUEBA,ARCHIVO:`
 - `OBJECTS=' " "D:\PRUEBA,ARCHIVO" " ' '`

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar `/home/archivo 2`, `/home/archivos gif` y `/home/archivo de prueba`, escriba:
 - `OBJECTS=' "/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba" '`
- Para especificar `/home/archivo de prueba`, escriba:
 - `OBJECTS=' "/home/archivo de prueba" '`

Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

Wait

Especifica si debe esperarse hasta que se complete una operación de cliente planificada. Este parámetro es útil cuando se definen las acciones de cliente de un script de mandatos o una macro. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que no esperará hasta que se haya completado la operación de cliente planificada. Si especifica este valor y el valor del parámetro ACTION es COMMAND, el código de retorno indicará si se ha definido o no la acción de cliente.

Yes

Especifica que esperará hasta que se haya completado la operación de cliente planificada. Si especifica este valor y el valor del parámetro ACTION es COMMAND, el código de retorno indicará el estado de la operación de cliente.

No puede emitir el mandato DEFINE CLIENTACTION con WAIT=YES desde la consola del servidor. Sin embargo, desde la consola del servidor podrá realizar lo siguiente:

- Especifique WAIT=YES con DEFINE CLIENTACTION como línea de mandatos de un mandato DEFINE SCRIPT.
- Especifique WAIT=YES con DEFINE CLIENTACTION como línea de mandatos de un archivo cuyo contenido se leerá en el script que se ha definido con un mandato DEFINE SCRIPT.

Restricción: Si especifica el mandato DEFINE CLIENTACTION con WAIT=YES en una macro, las planificaciones inmediatas que se han definido mediante el mandato no se retrotraerán si la macro no se completa correctamente.

Ejemplo: realizar una copia de seguridad incremental única

Emitir un mandato de copia de seguridad incremental para el nodo cliente TOM que está asignado al dominio de políticas EMPLOYEE_RECORDS. IBM Spectrum Protect define una planificación y la asocia al nodo de cliente TOM (se presupone que el planificador del cliente está en ejecución).

```
define clientaction tom domain=employee_records
action=incremental
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE CLIENTACTION

Mandato	Descripción
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
SET CLIENTACTDURATION	Especifica la duración de una planificación definida utilizando el mandato DEFINE CLIENTACTION.

DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)

Utilice este mandato para agregar una opción de cliente a un conjunto de opciones.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-DEFine CLIENTOpt--nombre_conjunto_opciones--nombre_opción--valor_opción-->
  .-Force---No-----
>+-----+-----<
```

```
'-Force-----No--+' '-SEQnumber-----number-'
'-Yes-'
```

Parámetros

nombre_conjunto_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones.

nombre_opción (Obligatorio)

Especifica la opción de cliente que se agrega al conjunto de opciones.

Consulte el apartado Opciones de cliente que puede establecer el servidor para obtener una lista de las opciones válidas.

Nota: Para definir valores de inclusión/exclusión, especifique la opción de inclusión o exclusión con *nombre_opción*, y utilice *valor_opción* para especificar las sentencias de inclusión o exclusión válidas, como lo haría en el archivo de opciones. Por ejemplo:

```
define clientopt nombre_conjunto_opciones inclexcl
"include c:\proj\text\devel.*"
```

valor_opción (Obligatorio)

Especifica el valor de la opción. Si la opción contiene más de un valor, éstos deben delimitarse por comillas.

Nota:

1. Las opciones QUIET y VERBOSE no tienen un valor de opción en el archivo de opciones del cliente. Para especificar estos valores en un conjunto de opciones de cliente del servidor, especifique el valor YES o NO.
2. Para añadir una opción INCLUDE o EXCLUDE para un nombre de archivo que contiene uno o más espacios, escriba la especificación de archivo entre comillas simples y la opción completa entre comillas dobles. Consulte el apartado Ejemplo: añadir una opción a un conjunto de opciones de cliente para obtener más información.
3. El valor de *valor_opción* está limitado a 1.024 caracteres.

Force

Especifica si el servidor fuerza al cliente a utilizar el valor de conjunto de opciones. El valor no se tiene en cuenta con las opciones aditivas como, por ejemplo, INCLEXCL y DOMAIN. El valor predeterminado es NO. Este parámetro es opcional. Los valores son:

Yes

Especifica que el servidor impone forzosamente al cliente la utilización del valor. (El cliente no puede alterar temporalmente el valor.)

No

Especifica que el servidor no impone forzosamente al cliente la utilización del valor. (El cliente sí puede alterar temporalmente el valor.)

SEQnumber

Especifica un número de secuencia cuando se especifica un nombre de opción más de una vez. Este parámetro es opcional.

Ejemplo: añadir una opción a un conjunto de opciones de cliente

Agregar una opción de cliente (MAXCMDRETRIES 5) a un conjunto de opciones de cliente denominado ENG.

```
define clientopt eng maxcmdretries 5
```

Ejemplo: añadir una opción para excluir un archivo de la copia de seguridad

Añadir una opción de cliente al conjunto de opciones ENGBACKUP para excluir el archivo c:\admin\file.txt de los servicios de copia de seguridad.

```
define clientopt engbackup inclexcl "exclude c:\admin\file.txt"
```

Ejemplo: añadir una opción para excluir un directorio de la copia de seguridad

Agregar una opción de cliente al conjunto de opciones WINSPEC para excluir un directorio temporal de Internet de los servicios de copia de seguridad. Cuando utilice la opción EXCLUDE o INCLUDE con nombres de archivo que contienen espacios, escriba la especificación de archivo entre comillas simples y la opción completa entre comillas dobles.

```
define clientopt winspec inclexcl "exclude.dir '*:\...\Temporary
Internet Files'"
```

Ejemplo: añadir una opción a los archivos de enlace en los directorios especificados

Añadir opciones de cliente al conjunto de opciones WINSPEC para enlazar todos los archivos de los directorios C:\Data y C:\Archivos de programa\My Apps con una clase de gestión denominada PRODCLASS.

```
define clienopt winspec inclexcl "include C:\Data\...\* prodclass"  
define clienopt winspec inclexcl "include 'C:\Archivos de  
programa\My Apps\...\*' prodclass"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE CLIENTOPT

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)

Utilice este mandato para definir un nombre para un conjunto de opciones que puede asignar a los clientes para las operaciones de archivado, copia de seguridad, restauración y recuperación.

Para añadir opciones al nuevo conjunto, ejecute el mandato DEFINE CLIENTOPT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-DEfine CLOptset--nombre_conjunto_opciones----->  
>--+-----+-----<  
'-DESCRiption----descripción-'
```

Parámetros

nombre_conjunto_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente. La longitud máxima del nombre es de 64 caracteres.

DESCRiption

Especifica una descripción del conjunto de opciones de cliente. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar encerrada entre comillas si contiene espacios en blanco. Este parámetro es opcional.

Ejemplo: definir un conjunto de opciones de cliente

Para definir un conjunto de opciones de cliente denominado ENG, emita el mandato siguiente:

```
define cloptset eng
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE CLOPTSET

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

DEFINE COLLOGROUP (Definir un grupo de proximidad)

Utilice este mandato para definir un grupo de proximidad. Un *grupo de proximidad* es un grupo de nodos o espacios de archivos en un nodo cuyos datos se colocan en un número mínimo de volúmenes de acceso secuencial. Sus datos se asignan sólo si la definición de la agrupación de almacenamiento está establecida como proximidad por grupo (COLLOCATE=GROUP).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine COLLOGGroup--nombre_grupo----->
>--+-----+-----><
  '-DESCRiption---'--descripción-'
```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad que desea crear. La longitud máxima del nombre es de 30 caracteres.

DESCRiption

Especifica una descripción del grupo de proximidad. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Definir un grupo de proximidad

Para definir un grupo de proximidad de espacio de archivos o nodo denominado GROUP1, emita el mandato siguiente:

```
define collogroup group1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE COLLOGGROUP

Mandato	Descripción
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.

Mandato	Descripción
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

DEFINE COLLOCMEMBER (Definir un miembro de grupo de proximidad)

Emita este mandato para agregar un nodo de cliente a un grupo de proximidad o para agregar un espacio de archivos de un nodo a un grupo de proximidad. Un grupo de proximidad es un grupo de nodos o espacios de archivos en un nodo cuyos datos se colocan en un número mínimo de volúmenes de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

Agregar un nodo a un grupo de proximidad

```

      .-,------.
      v          |
>>-DEFine COLLOCMember--nombre_grupo----nombre_nodo+-----><

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad al que desea agregar un nodo de cliente.

nombre_nodo

Especifica el nombre del nodo de cliente que desea agregar al grupo de proximidad. Puede especificar uno o más nombres.

Separe varios nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres.

Agregar un espacio de archivos de un nodo a un grupo de proximidad

```

>>-DEFine COLLOCMember--nombre_grupo--nombre_nodo----->
      .-,------.
      v          |
>>-FIlespace-----nombre_espacio_archivos+----->
      .-NAMEType-----SERVER-----
>+-----+-----+-----+----->
  '-NAMEType-----+SERVER--+
      +-UNICODE--+
      '-FSID----'
      .-CODEType-----BOTH-----
>+-----+-----+-----+-----><
  '-CODEType-----+BOTH-----+
      +-UNICODE-----+
      '-NONUNICODE-'

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad al que desea agregar un espacio de archivos.

nombre_nodo

Especifica el nodo de cliente donde se encuentra el espacio de archivos.

Filespace

Especifica el *nombre_espacio_archivos* en el nodo de cliente que desea agregar al grupo de proximidad. Puede especificar uno o más nombres de espacio de archivos que se encuentren en un nodo de cliente específico. Si especifica varios nombres de espacio de archivos, separe los nombres con comas sin espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres de espacio de archivos. Por ejemplo:

```
define collocmember manufacturing linux237 filespace=*_linux_fs
```

Este mandato coloca todos los espacios de archivos en el nodo linux237 con un nombre que acaba con *_linux_fs* en el grupo de proximidad manufacturing.

Consulte la lista siguiente para obtener sugerencias sobre cómo trabajar con grupos de proximidad:

- Al agregar miembros a un nuevo grupo de proximidad, el tipo del primer miembro del grupo de proximidad determina el tipo del grupo de proximidad. El grupo puede ser un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.
Restricción: Una vez que se ha establecido el tipo del grupo de proximidad, este no se puede cambiar.
- No puede mezclar tipos de miembro de grupo de proximidad al agregar miembros a un grupo de proximidad (un grupo de nodos o un grupo de espacios de archivos).
- Para un grupo de proximidad de espacio de archivos, puede agregar espacios de archivos al grupo. Los espacios de archivos deben utilizar el mismo valor que el parámetro *nombre_nodo* que se ha especificado al establecer el grupo de proximidad.
- Se puede incluir un nodo de cliente en varios grupos de espacios de archivos. Sin embargo, si un nodo es miembro de un grupo de proximidad de nodo, no puede ser miembro de un grupo de proximidad de espacio de archivos.
- Un espacio de archivos puede ser miembro de solo un grupo de espacios de archivos.

NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Especifique este parámetro cuando el servidor se comunique con clientes que tengan soporte de Unicode. Un cliente de copia de seguridad/archivado con soporte de Unicode solamente está disponible para los sistemas Windows, Macintosh OS 9, Macintosh OS X y NetWare. El nombre de espacio de archivos no puede ser un carácter comodín cuando se especifica NAMETYPE para un grupo de asignación de espacio de archivos. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión del nombre depende de los caracteres que contienen realmente los nombres y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos por sus ID de espacio de archivos (FSID).

CODETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro cuando utilice un carácter comodín para el nombre de espacio de archivos. Por ejemplo:

```
define collocmember production Win_3419 filespace=* codetype=unicode
```

Este mandato de ejemplo agrega todos los espacios de archivos del nodo Win_3419 al grupo de proximidad de producción. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Puede especificar uno de los siguientes valores:

BOTH

Incluir los espacios de archivos independientemente del tipo de página de códigos.

UNICODE

Incluir los espacios de archivos que solo están en Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en Unicode.

Definir dos miembros de grupo de proximidad

Definir dos miembros, NODE1 y NODE2, para un grupo de proximidad, GROUP1.

```
define collocmember group1 node1,node2
```

Definir un miembro de grupo de espacios de archivos CNTR90524, en el nodo clifton al grupo de proximidad TSM_alpha_1

```
define collocmember TSM_alpha_1 clifton filespace=CNTR90524
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE COLLOCMEMBER

Mandato	Descripción
DEFINE COLLOGGROUP	Define un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

DEFINE COPYGROUP (Definir un grupo de copia)

Utilice este mandato para definir un nuevo grupo de copia de seguridad o de copia archivada en una clase de gestión, un juego de políticas y un dominio de políticas específicos. El servidor utiliza los grupos de copia de seguridad y de copia archivada para controlar cómo hacen copias de seguridad y copias archivadas los clientes, y para gestionar las copias de seguridad y las copias archivadas.

Para que los clientes puedan utilizar el nuevo grupo de copia, debe activar el juego de políticas que contiene el nuevo grupo de copia.

Puede definir un grupo de copia archivada y un grupo de copia de seguridad para cada clase de gestión. Para asegurarse de que los nodos cliente pueden hacer copias de seguridad, incluya un grupo de copia de seguridad en la clase de gestión predeterminada de un juego de políticas.

Atención: El mandato DEFINE COPYGROUP no se ejecutará correctamente si especifica como destino una agrupación de almacenamiento de copia.

El mandato DEFINE COPYGROUP tiene dos formatos, uno para definir un grupo de copia de seguridad y otro para definir un grupo de copia archivada. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con DEFINE COPYGROUP

Mandato	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
SET ARCHIVERETENTIONPROTECTION	Especifica si la protección de retención de datos está activada.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

- DEFINE COPYGROUP (Definir un grupo de copia de seguridad)
Utilice este mandato para definir un nuevo grupo de copia de seguridad en una clase de gestión, un juego de políticas y un dominio de políticas específicos.
- DEFINE COPYGROUP (Definir un grupo de copias archivadas)
Utilice este mandato para definir un nuevo grupo de copia archivada en una clase de gestión, un juego de políticas y un dominio de políticas específicos.

DEFINE COPYGROUP (Definir un grupo de copia de seguridad)

Utilice este mandato para definir un nuevo grupo de copia de seguridad en una clase de gestión, un juego de políticas y un dominio de políticas específicos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

Sintaxis

```

>>-DEFine COpygroup--domain_name--policy_set_name--class_name-->
  .-STANDARD-.   .-Type----Backup-.
>-----+-----+-----+-----+-----+-----+----->
  '-STANDARD-'   '-Type----Backup-'

                                     .-FREquency----0----.
>--DESTination----nombre_agrupación--+-----+-----+----->
                                     '-FREquency----días-'

  .-VERExists----2----- .
>-----+-----+-----+-----+-----+-----+----->
  '-VERExists----+número--+-'
                                     '-NOLimit-'

  .-VERDeleted----1----- .
>-----+-----+-----+-----+-----+-----+----->
  '-VERDeleted----+número--+-'
                                     '-NOLimit-'

```

```

.-RETEExtra-----30----- .-RETOOnly-----60-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-RETEExtra-----+días-----+' '-RETOOnly-----+días-----+'
          '-NOLimit-'          '-NOLimit-'

.-MODE-----MODified-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-MODE-----+MODified--+'
          '-ABSolute-'

.-SERialization-----SHRStatic-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-SERialization-----+SHRStatic--++'
                          +-Static-----+
                          +-SHRDynamic--+
                          '-DYNAMIC----+'

>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
'-TOCDestination-----nombre_agrupación----'

```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas para el que está definiendo el grupo de copia.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas para el que está definiendo el grupo de copia.

No puede definir un grupo de copia para una clase de gestión que pertenezca al juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica la clase de gestión para la que está definiendo el grupo de copia.

STANDARD

Especifica el nombre del grupo de copia, que debe ser STANDARD. Este parámetro es opcional. El valor predeterminado es STANDARD.

Type=Backup

Especifica que desea definir un grupo de copia de seguridad. El parámetro predeterminado es BACKUP. Este parámetro es opcional.

DESTination (Obligatorio)

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los datos de copia de seguridad. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency

Especifica la frecuencia con la que IBM Spectrum Protect puede hacer copia de seguridad de un archivo. Este parámetro es opcional. IBM Spectrum Protect sólo hace copia de seguridad de un archivo cuando ha transcurrido el número de días desde la última copia de seguridad. El valor de FREQUENCY sólo se utiliza durante una operación de copia de seguridad incremental. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que IBM Spectrum Protect puede hacer copia de seguridad de un archivo independientemente del momento en que se hizo la última copia de seguridad del archivo.

VERExists

Especifica el número máximo de versiones de copia de seguridad para retener los archivos que actualmente se encuentran en el sistema de archivos del cliente. Este parámetro es opcional. El valor predeterminado es 2.

Si una operación de copia de seguridad incremental hace que se sobrepase el límite, el servidor hará que caduque la versión de copia de seguridad más antigua que existe en el almacenamiento del servidor. Los valores posibles son:

número

Especifica el número de versiones de copia de seguridad a retener para los archivos que actualmente se encuentran en el sistema de archivos del cliente. Puede especificar un entero de 1 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 2. Los valores preferidos son 3, 4, o más.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad.

El número de versiones de copia de seguridad que se retienen se controla mediante este parámetro hasta que las versiones sobrepasen el tiempo de retención que especifica el parámetro RETEXTRA.

VERDeleted

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad utilizando IBM Spectrum Protect. Este parámetro es opcional. El valor predeterminado es 1.

Si un usuario suprime un archivo del sistema de archivos del cliente, la siguiente copia de seguridad incremental hará que el servidor caduque las versiones más antiguas del archivo que sobrepasen este número. La fecha de caducidad de las versiones restantes se determina mediante el tiempo de retención especificado en los parámetros RETEXTRA y RETONLY. Los valores posibles son:

número

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad de los archivos que se han suprimido del sistema de archivos del cliente después de hacerse la copia de seguridad.

RETEExtra

Especifica el número de días que se ha de retener una versión de copia de seguridad una vez que esa versión se convierte en inactiva. Una versión de un archivo se convierte en inactiva cuando el cliente almacena otra copia de seguridad más reciente o cuando el cliente suprime el archivo de la estación de trabajo y luego ejecuta una copia de seguridad incremental completa. El servidor suprime las versiones inactivas basándose en el tiempo de retención aunque el número de versiones inactivas no sobrepase el número que permiten los parámetros VEREXISTS o VERDELETED. Este parámetro es opcional. El valor predeterminado es 30 días. Los valores posibles son:

días

Especifica el número de días que se retienen las versiones de copia de seguridad inactivas. Puede especificar un entero de 0 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 14 días. El valor preferido es 30 días o más.

NOLimit

Especifica que las versiones de copia de seguridad inactivas se retienen de forma indefinida.

Si especifica NOLIMIT, el servidor suprimirá las versiones de copia de seguridad inactivas basándose en el parámetro VEREXISTS (si el archivo todavía existe en el sistema de archivos del cliente) o en el parámetro VERDELETED (si el archivo ya no existe en el sistema de archivos del cliente).

RETOOnly

Especifica el número de días que se retiene la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente. Este parámetro es opcional. El valor predeterminado es 60. Los valores posibles son:

días

Especifica el número de días que se retiene la última versión inactiva restante de un archivo. Puede especificar un entero de 0 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 30 días.

NOLimit

Especifica que se desea conservar la última versión inactiva restante de un archivo de forma indefinida.

Si especifica NOLIMIT, el servidor retiene la última versión de copia de seguridad restante para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor.

MODE

Especifica si IBM Spectrum Protect sólo hace copia de seguridad de un archivo si éste se ha modificado desde la última copia de seguridad o si la hace siempre que un cliente solicita una copia de seguridad. Este parámetro es opcional. El valor predeterminado es MODIFIED. Los valores posibles son:

MODified

Especifica que IBM Spectrum Protect sólo hace copia de seguridad del archivo si éste se ha modificado desde la última copia de seguridad. IBM Spectrum Protect considera que un archivo se ha modificado si se cumple algunas de las siguientes condiciones:

- La fecha de última modificación es diferente
- El tamaño del archivo es diferente
- El propietario del archivo es diferente
- Los permisos de los archivos son diferentes

ABSolute

Especifica que IBM Spectrum Protect hace copia de seguridad del archivo independientemente de que se haya modificado.

El valor de MODE sólo se utiliza en la copia de seguridad incremental completa. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial.

SERIALIZATION

Especifica cómo debe procesar IBM Spectrum Protect los archivos o directorios cuando éstos se modifican durante el proceso de copia de seguridad. Este parámetro es opcional. El valor predeterminado es SHRSTATIC. Los valores posibles son:

SHRSTATIC

Especifica que IBM Spectrum Protect sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. IBM Spectrum Protect intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo o directorio se modifica durante cada intento de copia de seguridad, IBM Spectrum Protect no hace la copia de seguridad.

STATIC

Especifica que IBM Spectrum Protect sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. IBM Spectrum Protect intenta efectuar la copia de seguridad una sola vez.

Las plataformas que no dan soporte a la opción STATIC toman de forma predeterminada el valor SHRSTATIC.

SHRDYNAMIC

Especifica que si se modifica un archivo o directorio durante un intento de copia de seguridad, IBM Spectrum Protect hace copia de seguridad del archivo o directorio durante el último intento aunque el archivo o directorio se esté modificando. IBM Spectrum Protect intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

DYNAMIC

Especifica que IBM Spectrum Protect realiza la copia de seguridad de un archivo o directorio en el primer intento, independientemente de que el archivo o directorio esté modificándose durante el proceso de copia de seguridad. Atención: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar la copia de seguridad de un archivo o directorio mientras están produciéndose modificaciones. Como consecuencia, la versión de copia de seguridad puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se restaura un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una versión de copia de seguridad solo si el archivo o directorio no se está modificando.

TOCDESTINATION

Especifica la agrupación de almacenamiento primaria en la que inicialmente se almacenará una tabla de contenido (TOC) para cualquier operación de copia de seguridad NDMP (protocolo de gestión de datos de red) u operación de juego de copias de seguridad para la que se genere una TOC. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino. La agrupación de almacenamiento que se especifique para el destino debe tener el formato de datos NATIVE o NONBLOCK. Para evitar que se produzcan retardos de montaje, se recomienda que la agrupación de almacenamiento tenga una clase de dispositivo DISK o DEVTYPE=FILE. La generación de la TOC es opcional en las operaciones de copia de seguridad NDMP, pero no está admitida en otras operaciones de copia de seguridad de imagen.

Si se solicita la creación de la TOC para una operación de copia de seguridad que utilice NDMP y la imagen está vinculada a una clase de gestión cuyo grupo de copia de seguridad no especifica un destino de TOC, el resultado de la operación dependerá del parámetro TOC de la operación de copia de seguridad.

- Si TOC=PREFERRED (el valor predeterminado), la copia de seguridad continuará sin crearse una TOC.
- Si TOC=YES, la copia de seguridad en su totalidad resultará anómala porque no puede crearse ninguna TOC.

Ejemplo: crear un grupo de copias de seguridad

Crear un grupo de copia de seguridad denominado STANDARD para la clase de gestión ACTIVEFILES del juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS. El destino de copia de seguridad se establecerá en BACKUPPOOL. El intervalo mínimo entre copias de seguridad se establecerá en tres días, independientemente de si se han modificado los archivos. Se retendrán hasta cinco versiones de copia de seguridad mientras el archivo exista en el sistema de archivos del cliente.

```
define copygroup employee_records
vacation activefiles standard type=backup
destination=backuppool frequency=3
verexists=5 mode=absolute
```

DEFINE COPYGROUP (Definir un grupo de copias archivadas)

Utilice este mandato para definir un nuevo grupo de copia archivada en una clase de gestión, un juego de políticas y un dominio de políticas específicos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

Sintaxis

```
>>-DEFine COpYgroup--domain_name--policy_set_name--class_name-->
  .-STANDARD-.
>--+-----+---Type----Archive----->
  '-STANDARD-'

                                     .-FREQuency----Cmd-.
>--DESTination----nombre_agrupación----->
                                     '-FREQuency----Cmd-'

  .-RETVer----365----- .-RETInit----CREAtion--.
>--+-----+-----+-----+----->
  '-RETVer----+días----+' '-RETInit----Event---'
    '-NOLimit-'

  .-RETMin----365----- .-MODE----ABSolute-.
>--+-----+-----+----->
  '-RETMin----días----' '-MODE----ABSolute-'

  .-SERialization----SHRStatic----- .
>--+-----+-----><
  '-SERialization----+SHRStatic--+-'
    +-Static-----+
    +-SHRDYnamic+
    '-DYnamic----'
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas para el que está definiendo el grupo de copia.

nombre_juego_políticas (Necesario)

Especifica el nombre del juego de políticas para el que está definiendo el grupo de copia.

No puede definir un grupo de copia para una clase de gestión que pertenezca al juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica el nombre de la clase de gestión para la que está definiendo el grupo de copia.

STANDARD

Especifica el nombre del grupo de copia, que debe ser STANDARD. Este parámetro es opcional. El valor predeterminado es STANDARD.

Type=Archive (Necesario)

Especifica que desea definir un grupo de copia archivada.

DESTination (Obligatorio)

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente la copia archivada. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency=Cmd

Especifica la frecuencia de copia, que debe ser CMD. Este parámetro es opcional. El valor predeterminado es CMD.

RETVer

Especifica el número de días que se ha de mantener una copia archivada. Este parámetro es opcional. El valor predeterminado es 365. Los valores posibles son:

días

Especifica la cantidad de tiempo que se mantiene la copia de un archivo. Puede especificar un entero entre 0 y 30.000. Consejo: Para asegurarse de que los datos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 30 días. La opción del servidor RETENTIONEXTENSION puede afectar a la retención del volumen si las siguientes condiciones son verdaderas:

- Especifique cero para el número de días
- La agrupación de almacenamiento de destino para el grupo de copia de archivo es una agrupación de almacenamiento SnapLock (RECLAMATIONTYPE=SNAPLOCK)

Si se cumplen las dos condiciones y la retención de volúmenes está definida por el valor de la opción del servidor RETENTIONEXTENSION. El valor de la opción del servidor RETENTIONEXTENSION también se aplica si los datos se han copiado o movido a la agrupación de almacenamiento SnapLock por un proceso del servidor como la migración, o mediante los mandatos MOVE DATA o MOVE NODEDATA.

NOLimit

Especifica que desea conservar una copia archivada de forma indefinida.

Si especifica NOLIMIT, el servidor retiene las copias archivadas para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor. Si especifica NOLIMIT, no puede especificar también EVENT en el parámetro RETINIT.

El valor del parámetro RETVER puede afectar a la clase de gestión a la que el servidor vincula un directorio de copia archivada. Si el cliente no utiliza la opción ARCHMC, el servidor vincula los directorios de copia archivada con la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor vincula los directorios de copia archivada con la clase de gestión que presente el período de retención más reducido.

El parámetro RETVER del grupo de copia archivada de la clase de gestión a la que un objeto está vinculado determina el criterio de retención de cada objeto. Consulte el mandato SET ARCHIVERETENTIONPROTECTION para obtener una descripción de la protección de datos.

Si la agrupación de almacenamiento primaria especificada en el parámetro DESTINATION pertenece a una clase de dispositivo Centera y la protección de datos está activada, el valor de RETVER se envía a Centera para la gestión de la retención. Consulte el mandato SET ARCHIVERETENTIONPROTECTION para obtener una descripción de la protección de datos.

RETInit

Especifica cuándo comienza el tiempo de retención especificado en el atributo RETVER. Este parámetro es opcional. Si define el valor RETINIT durante la creación del grupo de copias, no podrá modificarlo más adelante. El valor predeterminado es CREATION. Los valores posibles son:

CREATION

Especifica que el tiempo de retención especificado en el atributo RETVER comienza en el momento en que una copia archivada se almacena en el servidor de IBM Spectrum Protect.

EVENT

Especifica que el tiempo de retención especificado en el parámetro RETVER comienza en el momento en que una aplicación de cliente notifica al servidor de que se ha producido un evento de inicio de retención para la copia archivada. Si especifica RETINIT=EVENT, no puede especificar también RETVER=NOLIMIT.

Consejo: Puede especificar una espera de supresión en un objeto que se ha almacenado con RETINIT=EVENT y para el cual el evento no se ha producido. Si el evento se produce mientras el objeto está en espera de supresión, se inicia el período de retención, pero el objeto no se suprimirá mientras siga en espera de supresión.

RETMIn

Especifica el número mínimo de días que se conserva una copia archivada después de que se archiva. Este parámetro es opcional. El valor predeterminado es 365. Si especifica RETINIT=CREATION, este parámetro se pasa por alto.

MODE=ABSolute

Especifica que siempre se archiva un archivo cuando el cliente lo solicita. El valor de MODE debe ser ABSOLUTE. Este parámetro es opcional. El valor predeterminado es ABSOLUTE.

SERIALIZATION

Especifica cómo procesará IBM Spectrum Protect los archivos que se han modificado durante la operación de archivado. Este parámetro es opcional. El valor predeterminado es SHRSTATIC. Los valores posibles son:

SHRSTATIC

Especifica que IBM Spectrum Protect sólo hace copia archivada de un archivo si éste no se está modificando. IBM Spectrum Protect intenta efectuar una operación de archivado hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo se modifica durante el intento de archivado, IBM Spectrum Protect no archivará el archivo.

STATIC

Especifica que IBM Spectrum Protect sólo hace copia archivada de un archivo si éste no se está modificando. IBM Spectrum Protect intenta efectuar la operación de archivado una sola vez.

Las plataformas que no dan soporte a la opción STATIC toman de forma predeterminada el valor SHRSTATIC.

SHRDYNAMIC

Especifica que si se modifica el archivo durante un intento de archivar, IBM Spectrum Protect archivar  el archivo en el  ltimo intento aunque se est  modificando. IBM Spectrum Protect intenta la opci n de archivado del archivo hasta cuatro veces, en funci n del valor especificado en la opci n del cliente CHANGINGRETRIES.

Dynamic

Especifica que IBM Spectrum Protect realiza la copia archivada de un archivo en el primer intento, independientemente de si el archivo est  modific ndose durante el proceso de archivado.

Atenci n: Debe tener mucho cuidado al utilizar los valores SHRDynamic y Dynamic. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar una operaci n de archivado de un archivo mientras est n produci ndose modificaciones. Como consecuencia, la copia archivada puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se recupera un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicaci n que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina SERIALIZATION en el valor SHRStatic o Static para que IBM Spectrum Protect cree una copia de archivado s lo si no se est  modificando el archivo.

Ejemplo: definir un grupo de copias archivadas para la retenci n basada en eventos

Crear un grupo de copia archivada denominado STANDARD para la clase de gesti n EVENTMC del juego de pol ticas SUMMER del dominio de pol ticas PROG1. Establecer el destino de la copia archivada en ARCHIVEPOOL, donde la copia archivada permanecer  hasta que el servidor reciba una notificaci n de que se ha producido un evento para iniciar el tiempo de retenci n, tras lo cual la copia archivada se conservar  durante 30 d as. La copia archivada se conservar  durante un m nimo de 90 d as tras su almacenamiento en el servidor, independientemente de cu ndo se notifique al servidor de que se ha producido un evento para iniciar el tiempo de retenci n.

```
define copygroup prog1 summer eventmc standard type=archive
destination=archivepool retinit=event retver=30 retmin=90
```

DEFINE DATAMOVER (Definir un transportador de datos)

Utilice este mandato para definir un transportador de datos. Un transportador de datos es un dispositivo designado que acepta una solicitud de IBM Spectrum Protect para transferir datos. Un transportador de datos se puede utilizar para realizar operaciones de copia en el exterior.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DATAMover--nombre_transportador_datos----->
. -Type--- --NAS----- .
>--+-----+-----+-----+-----+-----+----->
|           (1) (2) |
' -Type--- --+NASCLUSTER-+----- '
      '-NASVSERVER-'

. -LLAddress--- --1000----- .
>--HLAddress--- --direcci n-----+-----+----->
      '-LLAddress--- --puerto_tcp-'

>--USERid--- --ID_usuario--PASsword--- --contrase a----->

. -ONLine--- --Yes----- .
>--+-----+-----+---DATAFormat--- --+NETAPPDump--+-----><
' -ONLine--- --+Yes--+ '          +-CELERRADump-+
      '-No-- '                  '-NDMPDump---- '

```

Notas:

1. Puede especificar TYPE=NASCLUSTER y TYPE=NASVSERVER solo en un sistema operativo AIX, Linux o Windows.
2. Puede especificar TYPE=NASCLUSTER y TYPE=NASVSERVER s lo si DATAFORMAT=NETAPPDUMP.

Par metros

nombre_transportador_datos (Obligatorio)

Especifica el nombre del transportador de datos. Este nombre debe ser el mismo que el nombre de nodo con el que se ha registrado anteriormente mediante el mandato `REGISTER NODE TYPE=NAS`. Los datos de los que se hace copia de seguridad en este transportador de datos NAS se asignarán a este nombre de nodo en la base de datos del servidor. La longitud máxima permitida de este nombre es 64 caracteres.

Type

Especifica el tipo de transportador de datos. Este parámetro es opcional. El valor predeterminado es NAS.

NAS

Especifica que el transportador de datos es un servidor de archivos NAS.

NASCLUSTER

Especifica que el transportador de datos es un servidor de archivos NAS en clúster.

Restricción: Puede especificar el valor NASCLUSTER sólo si `DATAFORMAT=NETAPPDUMP`.

NASVSERVER

Especifica que el transportador de datos es un dispositivo de almacenamiento virtual dentro de un clúster.

Restricción: Puede especificar el valor NASVSERVER sólo si `DATAFORMAT=NETAPPDUMP`.

HLAddress (Obligatorio)

Especifica la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS.

Consejo: Para determinar la dirección IP numérica, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener la dirección.

LLAddress

Especifica el número de puerto TCP para acceder al dispositivo NAS para sesiones con el protocolo NDMP (Network Data Management Protocol). Este parámetro es opcional. El valor predeterminado es 10000.

USERid (Obligatorio)

Especifica el ID de un usuario autorizado para iniciar una sesión con el servidor de archivos NAS. Por ejemplo, especifique el ID de usuario que se ha configurado en el servidor de archivos NetApp para las conexiones NDMP.

Consejo: Para determinar el ID de usuario, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener el ID de usuario.

PASsword (Obligatorio)

Especifica la contraseña del ID de usuario para iniciar una sesión en el servidor de archivos NAS.

Consejo: Para determinar la contraseña, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener la contraseña.

ONLine

Especifica si el transportador de datos está disponible para utilizarlo. Este parámetro es opcional. El valor predeterminado es YES.

Yes

Es el valor predeterminado. Especifica que el transportador de datos está disponible para utilizarlo.

No

Especifica que el transportador de datos no está disponible para utilizarlo. Mientras se realicen las operaciones de mantenimiento de hardware, puede utilizar el mandato `UPDATE DATAMOVER` para desactivar el transportador de datos.

si se controla una biblioteca mediante una ruta desde un transportador de datos NAS a la biblioteca y el transportador de datos NAS está desactivado, el servidor no puede acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras el transportador de datos NAS está desactivado, no se inicializará la biblioteca.

DATAFormat (Obligatorio)

El formato de datos utilizado por este transportador de datos.

NETAPPDump

Se debe utilizar para los servidores de archivos NAS NetApp y para la serie N de IBM® System Storage.

CELERRADump

Se debe utilizar para los servidores de archivos NAS EMC Celerra.

NDMPDump

Se debe utilizar para los servidores de archivos NAS distintos de los servidores de archivos NetApp o EMC.

Ejemplo: definir un transportador de datos mediante un nombre de dominio

Definir un transportador de datos para el nodo denominado NAS1. El nombre de dominio del transportador de datos es NETAPP2.EXAMPLE.COM en el puerto 10000.

```
define datamover nas1 type=nas hladdress=netapp2.example.com lladdress=10000
userid=root password=admin dataformat=netappdump
```

Ejemplo: definir un transportador de datos mediante una dirección IP

Defina un transportador de datos para el nodo denominado NAS2. La dirección IP numérica para el transportador de datos es 203.0.113.0 en el puerto 10000. El servidor de archivos NAS no es un servidor de archivos NetApp ni EMC.

```
define datamover nas2 type=nas hladdress=203.0.113.0 lladdress=10000
  userid=root password=admin dataformat=ndmpdump
```

Ejemplo: definir un transportador de datos para un servidor de archivos en clúster mediante una dirección IP

Defina un transportador de datos para el servidor de archivos en clúster denominado NAS3. El servidor de archivos NAS es un dispositivo NetApp. La dirección IP numérica para el transportador de datos es 198.51.100.0 en el puerto 10000.

```
define datamover nas3 type=nascluster hladdress=198.51.100.0
  lladdress=10000 userid=root password=admin dataformat=netappdump
```



Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE DATAMOVER

Mandato	Descripción
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DATAMOVER	Suprimir un transportador de datos.
QUERY DATAMOVER	Visualiza definiciones de transportador de datos.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

DEFINE DEVCLASS (Definir una clase de dispositivo)

Utilice este mandato para definir una clase de dispositivo para un tipo de dispositivo de almacenamiento. El servidor exige que se defina una clase de dispositivo para poder utilizar un dispositivo.



Para ver la lista más actualizada de dispositivos soportados y los formatos válidos de las clases de dispositivo, consulte el sitio web Dispositivos soportados de IBM Spectrum Protect:  Sistemas operativos AIX  Sistemas operativos Windows

- Dispositivos compatibles con AIX y Windows

 Sistemas operativos Linux

- Dispositivos compatibles con Linux

Nota: La clase de dispositivo DISK la define IBM Spectrum Protect y no puede modificarse con el mandato DEFINE DEVCLASS.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS).

Las siguientes clases de dispositivo de IBM Spectrum Protect se ordenan por tipo de dispositivo.



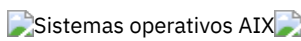
- DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
- DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
- DEFINE DEVCLASS (Definir una clase de dispositivo 4MM)
- DEFINE DEVCLASS (Definir una clase de dispositivo 8MM)
- DEFINE DEVCLASS (Definir una clase de dispositivo CENTERA)
- DEFINE DEVCLASS (Definir una clase de dispositivo DLT)
- DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE)
- DEFINE DEVCLASS (Definir una clase de dispositivo FILE)
-  Sistemas operativos AIX  Sistemas operativos Windows DEFINE DEVCLASS (Definir una clase de dispositivo GENERICTAPE)
- DEFINE DEVCLASS (Definir una clase de dispositivo LTO)
- DEFINE DEVCLASS (Definir una clase de dispositivo NAS)
- DEFINE DEVCLASS (Definir una clase de dispositivo REMOVABLEFILE)
- DEFINE DEVCLASS (Definir una clase de dispositivo SERVER)
- DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE)

Tabla 1. Mandatos relacionados con DEFINE DEVCLASS

Mandato	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.

DEFINE DEVCLASS (Definir una clase de dispositivo 3590)

Utilice la clase de dispositivo 3590 cuando utilice dispositivos de cinta 3590.

 Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo 3590 para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEfine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----3590----->
  .-FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+----->
  '-FORMAT----+DRIVE----+' '-ESTCAPacity---tamaño-'
      +-3590B----+
      +-3590C----+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'

  .-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+----->
  '-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

  .-MOUNTRetention---60----- .-MOUNTWait---60-----
>+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

  .-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+----->
  '-MOUNTLimit----+DRIVES-+'
      +-numero-+
      '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=3590 (Necesario)

Especifica que se asigna el tipo de dispositivo 3590 a la clase de dispositivo. 3590 indica que los dispositivos de cartuchos de cinta IBM® 3590 se asignan a esta clase de dispositivo.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En las tablas siguientes se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3590:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para 3590

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3590B	10 GB	Formato sin comprimir (básico)
3590C	Consulte la nota 20 GB	Formato comprimido
3590E-B	10 GB	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Consulte la nota 20 GB	Formato comprimido, similar al formato 3590C
3590H-B	30 GB (cartucho J, longitud estándar) 60 GB (cartucho K, longitud ampliada)	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Consulte la nota 60 GB (cartucho J, longitud estándar) 120 GB (cartucho K, longitud ampliada)	Formato comprimido, similar al formato 3590C
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.		

Tabla 2. Selecciones de formato de grabación de dispositivos 3590

Dispositivo	Formato					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Lectura/ Grabación	Lectura/ Grabación	–	–	–	–
Ultra SCSI	Lectura/ Grabación	Lectura/ Grabación	–	–	–	–
3590E	Lectura/ Grabación	Lectura/ Grabación	Lectura/ Grabación	Lectura/ Grabación	–	–
3590H	Lectura/ Lectura	Lectura/ Lectura	Lectura/ Lectura	Lectura/ Lectura	Lectura/ Grabación	Lectura/ Grabación

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número



Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta

clase de dispositivo.
0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DEFINE DEVCLASS (Definir una clase de dispositivo 3592)

Utilice la clase de dispositivo 3592 cuando utilice dispositivos de cinta 3592.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEfINE DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----3592----->

                                     (1)
.-LBProtect----No----- .-WORM----No-----
>+-----+-----+-----+-----+-----+----->
'-LBProtect----+READWrite+-' '-WORM----+Yes+-'
      +-WRITEOnly+-          '-No--'
      '-No-----'

.-SCALECAPacity----100----. .-FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+----->
'-SCALECAPacity----+100+-' '-FORMAT----+DRIVE----+'
      +-90--+                +-3592-----+
      '-20--'                +-3592C----+
                              +-3592-2---+
                              +-3592-2C--+
                              +-3592-3---+
                              +-3592-3C--+
                              +-3592-4---+
                              +-3592-4C--+
                              +-3592-5---+
                              +-3592-5C--+
                              +-3592-5A--+
                              '-3592-5AC-'

>+-----+-----+-----+-----+-----+----->
'-ESTCAPacity----tamaño-'

.-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+----->
'-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention----60----- .-MOUNTWait----60-----
>+-----+-----+-----+-----+-----+----->
'-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'

.-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+----->
'-MOUNTLimit----+DRIVES+-'
      +-número+
      '-0-----'

                                     (1) (2)
.-DRIVEEncryption----ALLOW-----
>+-----+-----+-----+-----+-----+----->
'-DRIVEEncryption----+ON-----+'
      +-ALLOW----+
      +-EXTERNAL+
      '-0-----'
```

Notas:

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. Se admite el cifrado de unidad solo para la segunda generación de unidades 3592 o posteriores.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=3592 (Necesario)

Especifica que se asigna el tipo de dispositivo 3592 a la clase de dispositivo.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

El valor predeterminado es NO.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades IBM® 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.

Consulte la nota técnica 1634851, Información adicional sobre la opción LBProtect de IBM Spectrum Protect, para ver una explicación sobre cuándo utilizar el parámetro LBProtect.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Recuerde:

1. Para utilizar el soporte WORM 3592 en bibliotecas 3584, debe especificar el parámetro WORM. El servidor distingue entre volúmenes reutilizables WORM y distintos de WORM. Sin embargo, para utilizar el soporte WORM 3592 en bibliotecas 349X, también deberá establecer WORMSCRATCHCATEGORY en el mandato DEFINE LIBRARY. Para obtener detalles, consulte el apartado DEFINE LIBRARY (Definir una biblioteca).
2. Cuando WORM=Yes, el único valor válido para el parámetro SCALECAPACITY es 100.
3. Consulte a sus proveedores para saber si su hardware tiene el nivel de soporte apropiado.

SCALECAPacity

Especifica el porcentaje de la capacidad del medio que puede utilizarse para almacenar datos. Este parámetro es opcional. El valor predeterminado es 100. Los valores posibles son 20, 90 y 100.

Si el porcentaje de la capacidad de escala se establece en 100, se proporciona la capacidad máxima de almacenamiento. Si se establece en 20 se obtiene el tiempo de acceso más rápido.

Nota: El valor de la capacidad de escala sólo entra en vigor cuando se graban datos por primera vez en un volumen. Cualquier actualización de la clase de dispositivo de capacidad de escala no afecta a los volúmenes que ya tienen datos grabados hasta que el volumen se vuelve a poner en estado reutilizable.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3592.

Consejo: El nombre de formato se especifica como, por ejemplo, 3592-X, 3592-XC, 3592-XA, o 3592-XAC, donde X indica la generación de la unidad, C indica un formato comprimido, y A indica una unidad de archivado.

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para 3592

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3592	300 GB	Formato sin comprimir (básico)
3592C	Consulte la nota.	Formato comprimido
3592-2	500 GB	Cintas JA con formato sin comprimir (básico)
	700 GB	Cintas JB con formato sin comprimir (básico)
3592-2C	1,5 TB	Cintas JA con formato comprimido
	2,1 TB	Cintas JB con formato comprimido
3592-3	640 GB	Cintas JA con formato sin comprimir (básico)
	1 TB	Cintas JB con formato sin comprimir (básico)
3592-3C	1,9 TB	Cintas JA con formato comprimido
	3 TB	Cintas JB con formato comprimido
3592-4	400 GB	Cintas JB con formato sin comprimir (básico)
	1,5 TB	Cintas JB con formato sin comprimir (básico)
	3,1 TB	Cintas JC con formato sin comprimir (básico)

Formato	Capacidad estimada	Descripción
3592-4C	1,2 TB	Cintas JK con formato comprimido
	4,4 TB	Cintas JB con formato comprimido
	9,4 TB	Cintas JC con formato comprimido
3592-5 (Para unidades IBM TS1150 Modelo 3592 E08 con ID de producto 03592E08)	900 GB	Cintas JB con formato sin comprimir (básico)
	7000 GB	Cintas JC/JY con formato sin comprimir (básico)
	2000 GB	Cintas JL con formato sin comprimir (básico)
	10.000 GB	Cintas JD/JZ con formato sin comprimir (básico)
3592-5C (Para unidades IBM TS1150 Modelo 3592 E08 con ID de producto 03592E08)	Depende de la compresibilidad de datos	Cintas JK con formato comprimido
		Cintas JC/JY con formato comprimido
		Cintas JL con formato comprimido
		Cintas JD/JZ con formato comprimido
3592-5A (Para unidades IBM TS1155 Modelo 3592 55F con ID de producto 0359255F)	3.000 GB	Cintas JL con formato sin comprimir (básico)
	15.000 GB	Cintas JD/JZ con formato sin comprimir (básico)
3592-5AC (Para unidades IBM TS1155 Modelo 3592 55F con ID de producto 0359255F)	Depende de la compresibilidad de datos	Cintas JL con formato comprimido
		Cintas JD/JZ con formato comprimido

Nota: Si este formato utiliza la función de compresión de unidades de cintas, en función de la eficacia de la compresión, la capacidad real podría ser distinta a la capacidad estimada.

Importante: Para un rendimiento óptimo, evite combinar distintas generaciones de unidades en una única biblioteca SCSI. Si debe combinar distintas generaciones de unidades en una biblioteca SCSI, utilice una de las configuraciones especiales que se describen en el tema sobre la combinación de generaciones de medios 3592.

También se necesitan configuraciones especiales para combinar distintas generaciones de unidades 3592 en bibliotecas 349x y ACSLS.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es AD5M. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir).

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifrarán otros tipos de volúmenes, por ejemplo, juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos). Si especifica ON y activa el método de cifrado del sistema o de la biblioteca, no se permitirá el cifrado de unidades y las operaciones de copia de seguridad fallarán.

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa el método de cifrado del sistema o de la biblioteca.

EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad.

Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado.

En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado del sistema o de la biblioteca, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

DEFINE DEVCLASS (Definir una clase de dispositivo 4MM)

Utilice la clase de dispositivo 4MM cuando utilice dispositivos de cinta de 4 mm.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary----nombre_biblioteca--DEVType----4MM----->
  .-FORMAT----DRIVE-----
>--+-----+-----+-----+-----+-----+----->
  '-FORMAT-----+DRIVE--+' '-ESTCAPacity----tamaño-'
      +-DDS1--+
      +-DDS1C+
      +-DDS2--+
      +-DDS2C+
      +-DDS3--+
      +-DDS3C+
      +-DDS4--+
      +-DDS4C+
      +-DDS5--+
      +-DDS5C+
      +-DDS6--+
      '-DDS6C-'

  .-PREFIX----ADSM-----
>--+-----+-----+-----+-----+-----+----->
  '-PREFIX-----+ADSM-----+'
      '-prefijo_volumen_cinta-'

  .-MOUNTWait----60----- .-MOUNTRetention----60-----
>--+-----+-----+-----+-----+-----+----->
  '-MOUNTWait----minutos-' '-MOUNTRetention----minutos-'

  .-MOUNTLimit----DRIVES-----
>--+-----+-----+-----+-----+-----+-----><
  '-MOUNTLimit----+DRIVES--+'
      +-número+
      '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRary (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 4 mm que esta clase de dispositivo ha utilizado. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=4MM (Necesario)

Especifica que se asigna el tipo de dispositivo 4MM a la clase de dispositivo. La especificación 4MM indica que a esta clase de dispositivo se asignan dispositivos de cinta de 4 mm.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 4 mm:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para las cintas de 4 mm

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DDS1	2.6 GB (60 metros) 4.0 GB (90 metros)	Formato sin comprimir, sólo aplicable a cintas de 60 y 90 metros
DDS1C	Consulte la nota 1,3 GB (60 metros) 2,0 GB (90 metros)	Formato comprimido, sólo aplicable a cintas de 60 y 90 metros
DDS2	4 GB	Formato sin comprimir, sólo se aplica a cintas de 120 metros
DDS2C	Consulte la nota 8 GB	Formato comprimido, sólo se aplica a cintas de 120 metros
DDS3	12 GB	Formato sin comprimir, sólo se aplica a cintas de 125 metros
DDS3C	Consulte la nota 24 GB	Formato comprimido, sólo se aplica a cintas de 125 metros
DDS4	20 GB	Formato sin comprimir, sólo se aplica a cintas de 150 metros
DDS4C	Consulte la nota 40 GB	Formato comprimido, sólo se aplica a cintas de 150 metros
DDS5	36 GB	Formato sin comprimir cuando se utilizan medios DAT 72
DDS5C	Consulte la nota 72 GB	Formato comprimido cuando se utilizan medios DAT 72
DDS6	80 GB	Formato sin comprimir, cuando se utilizan medios DAT 160
DDS6C	Consulte la nota 160 GB	Formato comprimido, cuando se utilizan medios DAT 160

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 4 mm, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del nombre de archivo en el que el servidor graba las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DEFINE DEVCLASS (Definir una clase de dispositivo 8MM)

Utilice la clase de dispositivo 8MM cuando utilice dispositivos de cinta de 8 mm.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
--LIBRary---nombre_biblioteca--DEVType---8MM----->
.-WORM---No-----.-FORMAT---DRIVE-----.
>+-----+-----+-----+-----+-----+----->
'-WORM---+-No---+' '-FORMAT---+-DRIVE---+'
      '-Yes-'               +-8200---+
                          +-8200C---+
                          +-8500---+
                          +-8500C---+
                          +-8900---+
                          +-AIT---+
                          +-AITC---+
                          +-M2---+
                          +-M2C---+
                          +-SAIT---+
                          +-SAITC---+
                          +-VXA2---+
                          +-VXA2C---+
                          +-VXA3---+
                          '-VXA3C-'

>+-----+-----+-----+-----+-----+----->
'-ESTCAPacity---tamaño-'

.-PREFIX---ADSM-----.
>+-----+-----+-----+-----+-----+----->
'-PREFIX---+-ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention---60-----.-MOUNTWait---60-----.
>+-----+-----+-----+-----+-----+----->
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

.-MOUNTLimit---DRIVES-----.
>+-----+-----+-----+-----+-----+----->
'-MOUNTLimit---+-DRIVES---+'
      +-numero-+
      '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRary (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 8 mm que esta clase de dispositivo ha utilizado. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=8MM (Necesario)

Especifica que se asigna el tipo de dispositivo 8MM a la clase de dispositivo. La especificación 8MM indica que a esta clase de dispositivo se asignan dispositivos de cinta de 8 mm.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Nota: Si selecciona Yes, las únicas opciones disponibles para el parámetro FORMAT son:

- DRIVE
- AIT
- AITC

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 8 mm:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para cintas de 8 mm

Formato Tipo de medio	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
8200	2,3 GB	Formato sin comprimir (estándar) con cartuchos de cintas de 112 metros
8200C	Consulte la nota 3,5 GB 4,6 GB	Formato comprimido con cartuchos de cintas de 112 metros estándar
8500 15 m 15 m 15 m 54 m 54 m 54 m 112 m 112 m 112 m 160 m XL	Consulte la nota 600 MB 600 MB 600 MB 2,35 GB 2,35 GB 2,35 GB 5 GB o 10 GB 5 GB o 10 GB 5 GB o 10 GB 7 GB	Unidades (Lectura Grabación) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW)

Formato		Descripción
Tipo de medio	Capacidad estimada	
8500C	Consulte la nota	Unidades (Lectura Grabación)
15 m	1,2 GB	Eliant 820 (RW)
15 m	1,2 GB	Exabyte 8500/8500C (RW)
15 m	1,2 GB	Exabyte 8505 (RW)
54 m	4,7 GB	Eliant 820 (RW)
54 m	4,7 GB	Exabyte 8500/8500C (RW)
54 m	4,7 GB	Exabyte 8505 (RW)
112 m	5 GB o 10 GB	Eliant 820 (RW)
112 m	5 GB o 10 GB	Exabyte 8500/8500C (RW)
112 m	5 GB o 10 GB	Exabyte 8505 (RW)
160 m XL	7 GB	Eliant 820 (RW)
8900	Consulte la nota	Unidad (Lectura Grabación)
15 m	–	Mammoth 8900 (R)
54 m	–	Mammoth 8900 (R)
112 m	–	Mammoth 8900 (R)
160 m XL	–	Mammoth 8900 (R)
22 m	2,5 GB	Mammoth 8900 (RW)
125 m	–	Mammoth 8900 (RW con actualización)
170 m	40 GB	Mammoth 8900 (RW)
AIT	Consulte la nota	Unidad
SDX1–25C	25 GB	Unidades
SDX1–35C	35 GB	AIT, AIT2 y AIT3
SDX2–36C	36 GB	Unidades
SDX2–50C	50 GB	AIT, AIT2 y AIT3
SDX3–100C	100 GB	Unidades AIT2 y AIT3
SDX3X-150C	150 GB	Unidades AIT2 y AIT3
SDX4–200C	200 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	400 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5
AITC	Consulte la nota	Unidad
SDX1–25C	50 GB	Unidades
SDX1–35C	91 GB	AIT, AIT2 y AIT3
SDX2–36C	72 GB	Unidades
SDX2–50C	130 GB	AIT, AIT2 y AIT3
SDX3–100C	260 GB	Unidades AIT2 y AIT3
SDX3X-150C	390 GB	Unidades AIT2 y AIT3
SDX4–200C	520 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	1040 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5
M2	Consulte la nota	Unidad (Lectura Grabación)
75 m	20 GB	Mammoth II (RW)
150 m	40 GB	Mammoth II (RW)
225 m	60 GB	Mammoth II (RW)
M2C	Consulte la nota	Unidad (Lectura Grabación)
75 m	50 GB	Mammoth II (RW)
150 m	100 GB	Mammoth II (RW)
225 m	150 GB	Mammoth II (RW)

Formato Tipo de medio	Capacidad estimada	Descripción
SAIT	Consulte la nota 500 GB	Unidad (Lectura Grabación) Sony SAIT1-500(RW)
SAITC	Consulte la nota 1300 GB (1,3 TB)	Unidad (Lectura Grabación) Sony SAIT1-500(RW)
VXA2 V6 (62 m) V10 (124 m) V17 (170 m)	Consulte la nota 20 GB 40 GB 60 GB	Unidad (Lectura Grabación) VXA-2
VXA2C V6 (62 m) V10 (124 m) V17 (170 m)	Consulte la nota 40 GB 80 GB 120 GB	Unidad (Lectura Grabación) VXA-2
VXA3 X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 40 GB 86 GB 160 GB	Unidad (Lectura Grabación) VXA-3
VXA3C X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 80 GB 172 GB 320 GB	Unidad (Lectura Grabación) VXA-3
<p>Nota: Las capacidades reales pueden variar en función de los cartuchos y las unidades que se utilicen.</p> <ul style="list-style-type: none"> • Para el formato M2C, la proporción de compresión normal es de 2,5:1. • Para los formatos AITC y SAITC, la proporción de compresión normal es de 2.6:1. 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 8 mm, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADMS. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

Ejemplo: definir una clase de dispositivo de 8 mm

Definir una clase de dispositivo que se denomina 8MMTAPE para un dispositivo 8 mm en una biblioteca denominada AUTO. El formato es DRIVE, el límite de montaje es 2, la retención de montaje es 10, el prefijo del volumen de cinta se denomina ADSMVOL y la capacidad estimada es 6 GB.

```
define devclass 8mmtape devtype=8mm library=auto
format=drive mountlimit=2 mountretention=10
prefix=adsmvol estcapacity=6G
```

DEFINE DEVCLASS (Definir una clase de dispositivo CENTERA)

Utilice la clase de dispositivo CENTERA cuando utilice dispositivos de almacenamiento EMC Centera. El tipo de dispositivo CENTERA utiliza los archivos como volúmenes para almacenar los datos de forma secuencial. Es similar a la clase de dispositivo FILE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>-DEVType----CENTERA----->
      .-,'-----
      (1)  V  |
>-HLAddress-----dirección_ip+-?archivo_PEA----->
      .-MINCAPacity----100M---.  .-MOUNTLimit-----1-----
>+-----+-----+-----+-----><
  '-MINCAPacity----tamaño-'  '-MOUNTLimit----numero-'
```

Notas:

1. Para cada clase de dispositivo Centera, debe especificar una o varias direcciones IP. Sin embargo, la ruta y el nombre del archivo PEA (autorización de entrada de la agrupación) son opcionales, y una especificación del archivo PEA puede seguir a las direcciones IP. Utilice el carácter "?" para separar la ruta y el nombre de archivo PEA de las direcciones IP.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

DEVType=CENTERA (Necesario)

Especifica que se asigna el tipo de dispositivo Centera a esta clase de dispositivo. Todos los volúmenes pertenecientes a una agrupación de almacenamiento que está definida con esta clase de dispositivo son volúmenes lógicos que son un tipo de medio de acceso secuencial.

HLAddress


Especifica una o varias direcciones IP para el dispositivo de almacenamiento Centera y, opcionalmente, el nombre y la ruta de un archivo PEA (autorización de entrada de agrupación). Especifique las direcciones IP en formato decimal con punto (por ejemplo, 9.10.111.222). Un dispositivo Centera puede tener varias direcciones IP. Si se especifican varias direcciones IP, la operación de almacenamiento o recuperación intenta establecer una conexión utilizando cada dirección IP especificada hasta encontrar una dirección válida.

 Sistemas operativos AIX La ruta y el nombre del archivo PEA son sensibles a las mayúsculas y minúsculas.

Si añade el nombre y la ruta de un archivo PEA, asegúrese de que el archivo se almacena en un directorio del sistema que ejecuta el servidor. Separe el nombre y la ruta del archivo PEA de la dirección IP utilizando "?" como por ejemplo:

 Sistemas operativos Windows

```
HLADDRESS=9.10.111.222,9.10.111.223?c:\controlFiles\TSM.PEA
```

 Sistemas operativos AIX

```
HLADDRESS=9.10.111.222,9.10.111.223?/user/ControlFiles/TSM.PEA
```

Especifique sólo una ruta y nombre de archivo PEA para cada definición de clase de dispositivo. Si especifica dos clases de dispositivo Centera distintas que hagan referencia al mismo dispositivo de almacenamiento Centera y si las definiciones de clase de dispositivo contienen distintas rutas y nombres de archivo PEA, el servidor utiliza el archivo PEA especificado en el parámetro HLADDRESS de la clase de dispositivo que se haya utilizado en primer lugar para abrir el dispositivo de almacenamiento Centera. Consejos:

1. El servidor no incluye un archivo PEA durante la instalación. Si no crea ningún archivo PEA, el servidor utilizará el perfil predeterminado de Centera, que permite a las aplicaciones leer, escribir, suprimir, depurar y consultar datos de un dispositivo de almacenamiento Centera. Para conseguir un control más estricto, cree un archivo PEA utilizando la interfaz de línea de mandatos proporcionada por EMC Centera. Para obtener detalles sobre la autenticación y autorización de Centera, consulte la publicación *Programmer's Guide* de EMC Centera.

- También puede especificar la ruta y el nombre del archivo PEA en una variable de entorno utilizando la sintaxis CENTERA_PEA_LOCATION=rutaarchivo_nombrearchivo. La ruta y el nombre del archivo PEA especificados en esta variable de entorno se aplicarán a todos los clústeres de Centera. Si utiliza esta variable, no es necesario que especifique la ruta y el nombre del archivo PEA utilizando el parámetro HLADDRESS.

MINCAPacity

Especifica el tamaño mínimo para los volúmenes Centera que se asignan a una agrupación de almacenamiento de esta clase de dispositivo. Este valor representa la cantidad mínima de datos que se almacenan en un volumen Centera antes de que el servidor lo marque como lleno. Los volúmenes Centera seguirán aceptando datos hasta que se haya almacenado la cantidad mínima de datos. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor predeterminado es 100 MB (MINCAPACITY=100M). El valor mínimo permitido es 1 MB (MINCAPACITY=1M). El valor máximo permitido es 128 GB (MINCAPACITY=128G).

MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. El valor predeterminado es 1. Este parámetro es opcional. Puede especificar un número a partir de 0 o mayor; no obstante, la suma de todos los valores de límite de montaje para todas las clases de dispositivo asignadas al mismo dispositivo Centera no debe superar el número máximo de sesiones que permite Centera.

DEFINE DEVCLASS (Definir una clase de dispositivo DLT)

Utilice la clase de dispositivo DLT cuando utilice dispositivos de cinta DLT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY---nombre_biblioteca--DEVType---DLT----->
. -WORM----No----- . -FORMAT----DRIVE-----
>+-----+-----+-----+----->
' -WORM----+No--+-' ' -FORMAT----+DRIVE----+'
          '-Yes-'          +-DLT1-----+
                              +-DLT1C-----+
                              +-DLT10-----+
                              +-DLT10C----+
                              +-DLT15-----+
                              +-DLT15C----+
                              +-DLT20-----+
                              +-DLT20C----+
                              +-DLT35-----+
                              +-DLT35C----+
                              +-DLT40-----+
                              +-DLT40C----+
                              +-DLT2-----+
                              +-DLT2C-----+
                              +-DLT4-----+
                              +-DLT4C-----+
                              +-SDLT-----+
                              +-SDLTC-----+
                              +-SDLT320--+
                              +-SDLT320C--+
                              +-SDLT600--+
                              +-SDLT600C--+
                              +-DLTS4-----+
                              '-DLTS4C---+'
>+-----+-----+-----+----->
' -ESTCAPacity---tamaño-'
. -PREFIX----ADSM-----
>+-----+-----+-----+----->
' -PREFIX----+ADSM-----+'
          '-prefijo_volumen_cinta-'
```

```

.-MOUNTRetention====60----- .-MOUNTWait====60-----.
>-----+-----+-----+-----+-----+-----+----->
'-MOUNTRetention====minutos-' '-MOUNTWait====minutos-'

.-MOUNTLimit====DRIVES-----.
>-----+-----+-----+-----+-----+-----+-----><
'-MOUNTLimit====+DRIVES++'
      +-número+
      '-0-----'

```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta DLT utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=DLT (Necesario)

Especifica que se asigna el tipo de dispositivo DLT a la clase de dispositivo. DLT indica que se asignan dispositivos de cinta DLT a esta clase de dispositivo.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Nota: El soporte para los medios WORM de DLT sólo está disponible para las unidades SDLT-600, Quantum DLT-V4 y Quantum DLT-S4 en las bibliotecas manuales, SCSI y ACSLS.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos DLT:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para DLT

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DLT1	40 GB	Formato sin comprimir sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT1C	Consulte la nota 1. 80 GB	Formato comprimido sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT10	10 GB	Formato sin comprimir sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT10C	Consulte la nota 1. 20 GB	Formato comprimido sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT15	15 GB	Formato sin comprimir sólo con cartuchos CompacTape IIIxt Válido con unidades DLT4000, DLT7000 y DLT8000

Formato	Capacidad estimada	Descripción
DLT15C	Consulte la nota 1. 30 GB	Formato comprimido sólo con cartuchos CompacTape IIIxt Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20	20 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20C	Consulte la nota 1. 40 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT35	35 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT35C	Consulte la nota 1. 70 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT40	40 GB	Formato sin comprimir sólo con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT40C	Consulte la nota 1. 80 GB	Formato comprimido con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT2	80 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLTtape VS1
DLT2C	Consulte la nota 1. 160 GB	Formato comprimido, cuando se utilizan medios Quantum DLTtape VS1
DLT4	160 GB	Formato sin comprimir, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
DLT4C	Consulte la nota 1. 320 GB	Formato comprimido, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
SDLT Consulte la nota 2.	100 GB	Formato sin comprimir con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLTC Consulte la nota 2.	Consulte la nota 1. 200 GB	Formato comprimido con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLT320 Consulte la nota 2.	160 GB	Formato sin comprimir, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT320C Consulte la nota 2.	Consulte la nota 1. 320 GB	Formato comprimido, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT600	300 GB	Formato sin comprimir, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT
SDLT600C	Consulte la nota 1. 600 GB	Formato comprimido, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT
DLTS4	800 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4
DLTS4C	Consulte la nota 1. 1,6 TB	Formato comprimido, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4

Formato	Capacidad estimada	Descripción
<p>Nota:</p> <ol style="list-style-type: none"> 1. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista. 2. IBM Spectrum Protect no admite una biblioteca que contenga unidades SDLT BRC (Backward Read Compatible) y SDLT NBRC (Non-Backward Read Compatible). 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información sobre capacidades estimadas, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADMS. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADMS.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número



Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE)

Utilice la clase de dispositivo ECARTRIDGE cuando está utilizando unidades StorageTek tales como StorageTek T10000 o T9840.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFINE DEVclass--nombre_clase_dispositivo----->
>--LIBRARY---nombre_biblioteca--DEVType---ECARtridge----->
                                     (1)
.-LBProtect---No-----.-WORM---No-----
>-----+-----+-----+-----+-----+-----+----->
'-LBProtect---+READWrite++' '-WORM---+No---+'
          +-WRITEOnly-+          '-Yes-'
          '-No-----'

.-FORMAT---DRIVE-----
>-----+-----+-----+-----+-----+-----+----->
'-FORMAT---+DRIVE---+' '-ESTCAPacity---tamaño-'
          +-T9840C---+
          +-T9840C-C--+
          +-T9840D---+
          +-T9840D-C--+
          +-T10000A---+
          +-T10000A-C--+
          +-T10000B---+
          +-T10000B-C--+
          +-T10000C---+
          +-T10000C-C--+
          +-T10000D---+
          '-T10000D-C-'

.-PREFIX---ADSM-----
>-----+-----+-----+-----+-----+-----+----->
'-PREFIX---+ADSM-----+'
          '-prefijo_volumen_cinta-'

.-MOUNTRetention---60-----.-MOUNTWait---60-----.
```



```

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

.-MOUNTLimit---DRIVES----.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTLimit---+DRIVES++'
          +número+
          '-0-----'

          (1) (2)
.-DRIVEEncryption---ALLOW-----.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
'-DRIVEEncryption---+ON-----+'
          +-ALLOW----+
          +-EXternal-+
          '-OFF-----'

```

Notas:

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. Puede utilizar el cifrado de unidad solo en unidades Oracle StorageTek T10000B con un valor de formato de DRIVE, T10000B o T10000B-C, para unidades Oracle StorageTek T10000C con un valor de formato de DRIVE, T10000C o T10000C-C y para unidades Oracle StorageTek T10000D con un valor de formato de DRIVE, T10000D y T10000D-C.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas ECARTRIDGE que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=ECARTRidge (Necesario)

Especifica que se asigna el tipo de dispositivo ECARTRIDGE a la clase de dispositivo. ECARTRIDGE indica que se asigna un tipo específico de dispositivo de cartucho de cinta (StorageTek) a esta clase de dispositivo.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

El valor predeterminado es NO.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para

un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades Oracle StorageTek T10000C y Oracle StorageTek T10000D.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Restricción: Si selecciona Sí, las únicas opciones que están disponibles para el parámetro FORMAT son:

- DRIVE
- T9840C
- T9840C-C
- T9840D
- T9840D-C
- T10000A
- T10000A-C
- T10000B
- T10000B-C
- T10000C
- T10000C-C
- T10000D
- T10000D-C

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

Importante: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos ECARTRIDGE:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000

Formato	Capacidad estimada	Descripción
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Notas:</p> <ul style="list-style-type: none"> Algunos formatos utilizan la función de compresión por hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista. Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C. 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es AD\$M. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es AD\$M.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir).

Restricciones:

1. Solo puede utilizar el cifrado de unidad en las siguientes unidades:
 - Las unidades Sun StorageTek T10000B con un valor de formato DRIVE, T10000B o T10000B-C
 - Las unidades Sun StorageTek T10000C con un valor de formato DRIVE, T10000C o T10000C-C
 - Unidades Oracle StorageTek T10000D con un valor de formato DRIVE, T10000D o T10000D-C
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios de una sola grabación, varias lecturas (WORM). No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
3. Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

EXternal



Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.


OFF



Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

DEFINE DEVCLASS (Definir una clase de dispositivo FILE)

Utilice la clase de dispositivo FILE si utiliza archivos en el almacenamiento de disco magnético como volúmenes que almacenan datos secuencialmente (como en una cinta).

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo FILE no admite las bibliotecas EXTERNAL ni Remote Storage Manager.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEfINE DEVclass--nombre_clase_dispositivo----->
                                     .-MOUNTLimit---20----.
>--DEVType---FILE-+-----+----->
                                     '-MOUNTLimit---número-'

                                     .-MAXCAPacity---10G----.
>--+-----+----->
                                     '-MAXCAPacity---tamaño-'

                                     .-DIRectory---nombre_directorio_actual-.
>+-----+-----+----->
|                                     .-+-----+-----+-----+-----+
|                                     V                                     |
|                                     '-DIRectory---nombre_directorio-+-----'

                                     .-SHARED---No------.
>--+-----+-----+-----><
                                     '-SHARED---+No--+-'
                                     '-Yes-'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.


DEVType=FILE (Necesario)

Especifica que se asigna el tipo de dispositivo FILE a la clase de dispositivo. FILE indica que se asigna un archivo a esta clase de dispositivo. Cuando el servidor necesita acceder a un volumen que pertenece a esta clase de dispositivo, abre un archivo y lee o graba datos del archivo.

Un archivo es un formato de medio de acceso secuencial.

MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. Este parámetro es opcional. El valor predeterminado es 20. Puede especificar un número de 0 a 4096.

 Sistemas operativos Windows Si la clase de dispositivo se comparte con un agente de almacenamiento (mediante la especificación del parámetro SHARED=YES), se definirán o se suprimirán unidades en función del valor de límite de montaje.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor



del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

MAXCAPacity

Especifica el tamaño máximo de los archivos de almacenamiento de datos definidos en una agrupación de almacenamiento de esta clase de dispositivo.

El valor del parámetro MAXCAPACITY también se utiliza como unidad de asignación cuando el desencadenante de espacio de la agrupación de almacenamiento crea volúmenes. El valor predeterminado son 10 GB (MAXCAPACITY=10G). El valor especificado debe ser menor o igual que el tamaño máximo admitido de un archivo en el sistema de archivos destino.



Especifique este valor como un entero seguido de **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). Si está definiendo una clase de dispositivo FILE para los volúmenes de copia de seguridad de base de datos, especifique un valor para MAXCAPACITY que sea adecuado para el tamaño de la base de datos y que minimice el número de volúmenes de base de datos.


 Sistemas operativos AIX  Sistemas operativos Linux No defina un valor para MAXCAPACITY superior a 640M cuando este archivo se destine al soporte de CD REMOVABLEFILE. Un valor menor que un espacio utilizable del CD (650 MB) permite una coincidencia unívoca entre los archivos de la clase de dispositivo FILE y las copias que se encuentran en el CD.

DIRectory

Especifica las ubicaciones del directorio de los archivos utilizados en esta clase de dispositivo. Escriba comillas al principio y al final de la lista de directorios y utilice comas para separar los nombres de directorio individuales. Se permiten los caracteres especiales (por ejemplo, espacios en blanco) en los nombres de directorio. Por ejemplo, la lista de directorios "abc def,xyz" contiene dos directorios: abc def y xyz.



Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Linux El valor predeterminado es el directorio de trabajo actual del servidor que se utiliza en el momento en el que se emite el mandato.



 Sistemas operativos Windows El valor predeterminado es el directorio de trabajo actual del servidor que se utiliza en el momento en el que se emite el mandato. La información del registro de Windows se utiliza para determinar el directorio predeterminado.


Al especificar un nombre o nombres de directorio, identifica la ubicación donde el servidor coloca los archivos que representan los volúmenes de almacenamiento para esta clase de dispositivo.

Para el soporte de NetApp SnapLock (agrupaciones de almacenamiento con RECLAMATIONTYPE=SNAPLOCK, que van a utilizar esta clase de dispositivo), el directorio o directorios especificados con el parámetro DIRECTORY deben apuntar al directorio o directorios de los volúmenes NetApp SnapLock.

 Sistemas operativos AIX  Sistemas operativos Linux Al procesar el mandato, el servidor amplía el nombre o nombres de directorio especificados a forma completa, a partir del directorio raíz.

Si el servidor necesita asignar un volumen reutilizable, crea un nuevo archivo en uno de estos directorios. (El servidor puede elegir cualquiera de los directorios para crear nuevos volúmenes reutilizables.) Para los volúmenes reutilizables que se utilizan para almacenar datos del cliente, el archivo que crea el servidor tiene la extensión de nombre de archivo .bfs. Para los volúmenes reutilizables que se utilizan para almacenar datos de exportación, se utiliza la extensión .exp.

 Sistemas operativos AIX  Sistemas operativos Linux Por ejemplo, si define una clase de dispositivo con un directorio de tsmstor y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine /tsmstor/00566497.exp.

 Sistemas operativos Windows Por ejemplo, si define una clase de dispositivo con un directorio de c:\server y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine c:\server\00566497.exp.

Importante: Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Si el agente de almacenamiento no puede acceder al volumen FILE, puede hacer que las operaciones se reintenten en una ruta de sólo LAN o que fallen. Para obtener más información, consulte la descripción del parámetro DIRECTORY en el apartado DEFINE PATH (Definir una ruta).

Consejo: Si especifica varios directorios para una clase de dispositivo, asegúrese de que los directorios están asociados con sistemas de archivos separados. Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio agregando valores que representan el espacio que queda en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los

desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar inhabilitado. Si un desencadenante se inhabilita porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a habilitar el desencadenante con el siguiente mandato: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.


SHAREd

Especifica si esta clase de dispositivo FILE se compartirá entre el servidor y uno o más agentes de almacenamiento. Para prepararse para el compartimiento, se definirá de manera automática una biblioteca junto con un número de unidades correspondiente al valor del parámetro MOUNTLIMIT. Los nombres de unidad son el nombre de la biblioteca más un número comprendido entre 1 y el número de límite de montaje. Por ejemplo, si el nombre de la biblioteca es FILE y el límite de montaje está establecido en 4, las unidades se denominan FILE11, FILE12, FILE13 y FILE14.


Para obtener información acerca de los requisitos previos que deben aplicarse cuando el servidor y el agente de almacenamiento comparten el almacenamiento, consulte el sitio IBM® Support Portal for IBM Spectrum Protect.

Ejemplo: definir una clase de dispositivo FILE con varios directorios

Definir una clase de dispositivo que especifica varios directorios.

 Sistemas operativos AIX

```
define devclass multidir devtype=file
  directory=/usr/xyz,/usr/abc,/usr/uvw
```

 Sistemas operativos Linux

```
define devclass multidir devtype=file
  directory=/opt/xyz,/opt/abc,/opt/uvw
```

 Sistemas operativos Windows

```
define devclass multidir devtype=file
  directory=e:\xyz,f:\abc,g:\uvw
```

Ejemplo: definir una clase de dispositivo FILE con capacidad de 50 MB

Definir una clase de dispositivo denominada PLAINFILES con un tipo de dispositivo FILE y con una capacidad máxima de 50 MB.

```
define devclass plainfiles devtype=file
  maxcapacity=50m
```

 Sistemas operativos AIX  Sistemas operativos Windows

DEFINE DEVCLASS (Definir una clase de dispositivo GENERICTAPE)

Utilice la clase de dispositivo GENERICTAPE para las unidades de cinta admitidas por los controladores de dispositivo del sistema operativo.

Cuando se utiliza este tipo de dispositivo, el servidor no reconoce ningún tipo de dispositivo ni el formato de grabación de cartuchos. Dado que el servidor no reconoce el tipo de dispositivo, si se produce un error de E/S, la información de error será menos detallada en comparación con la información de error que se generaría para un tipo de dispositivo específico (por ejemplo, 8MM). Cuando defina dispositivos en el servidor, no combine varios tipos de dispositivos en el mismo tipo de dispositivo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY---nombre_biblioteca--DEVtype---GENERICTape----->
      .-MOUNTRetention----60-----.
>---+-----+-----+-----+-----+-----+----->
  '-ESTCAPacity---tamaño-' '-MOUNTRetention---minutos-'
```

```

.-MOUNTWait-----60----- .-MOUNTLimit-----DRIVES-----
>-----+-----+-----+-----+-----+-----+-----><
'-MOUNTWait-----minutos-' '-MOUNTLimit-----+DRIVES++-'
                                     +-número+
                                     '-0-----'

```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=GENERICtape (Obligatorio)

Especifica que se asigna el tipo de dispositivo GENERICTAPE a la clase de dispositivo. GENERICTAPE indica que los volúmenes de esta clase de dispositivo se utilizan en las unidades de cintas que admite el controlador de dispositivo de cintas del sistema operativo.

El servidor reconoce que el medio se puede eliminar y que se pueden insertar más medios, sujetos a límites establecidos con el parámetro MOUNTLIMIT para la clase de dispositivo y el parámetro MAXSCRATCH para la agrupación de almacenamiento.

Los volúmenes de una clase de dispositivo con un tipo de dispositivo GENERICTAPE son volúmenes de acceso secuencial.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Especifique una capacidad adecuada a la unidad de cintas determinada que esté utilizándose.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DEFINE DEVCLASS (Definir una clase de dispositivo LTO)

Utilice la clase de dispositivo LTO cuando utilice dispositivos de cinta LTO.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFINE DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----LTO----->
                                     (1)
.-LBProtect----No----- .-WORM----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-LBProtect----+READWrite+-' '-WORM----+No--+-'
      +WRITEOnly--+           '-Yes-'
      '-No-----'

.-FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-FORMAT----+DRIVE----+' '-ESTCAPacity----tamaño-'
      +-ULTRIUM---+
      +-ULTRIUMC--+
      +-ULTRIUM2--+
      +-ULTRIUM2C--+
      +-ULTRIUM3--+
      +-ULTRIUM3C--+
      +-ULTRIUM4--+
      +-ULTRIUM4C--+
      +-ULTRIUM5--+
      +-ULTRIUM5C--+
      +-ULTRIUM6--+
      '-ULTRIUM6C-'

.-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention----60----- .-MOUNTWait----60-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'

.-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTLimit----+DRIVES+-'
      +-numero--+
      '-0-----'
```


Nota:

1. para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben admitir medios WORM.
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.)

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

Cuando migre todas las unidades de dispositivos Ultrium a dispositivos Ultrium 2:

- Suprima todas las definiciones de unidades Ultrium existentes y las rutas asociadas a ellas.
- Defina las nuevas unidades y rutas Ultrium 2.

Si piensa en mezclar distintas generaciones de unidades y medios LTO, tenga en cuenta las siguientes restricciones.

Tabla 1. Posibilidades de lectura/grabación para diferentes generaciones de unidades LTO

Unidades	Soporte de primera generación	Soporte de segunda generación	Soporte de tercera generación	Soporte de cuarta generación	Soporte de quinta generación	Soporte de sexta generación
Primera generación	Lectura y grabación	n/d	n/d	n/d	n/d	n/d
Segunda generación	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d	n/d
Tercera generación ¹	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d
Cuarta generación ²	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d
Quinta generación ³	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d
Sexta generación ⁴	n/d	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación

¹ En una biblioteca con una unidad de tercera generación, es necesario dar de baja todos los volúmenes reutilizables de primera generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de primera generación a sólo lectura.

² En una biblioteca con una unidad de cuarta generación, es necesario dar de baja todos los volúmenes reutilizables de segunda generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de segunda generación a sólo lectura.

³ En una biblioteca con una unidad de quinta generación, todos los volúmenes reutilizables de tercera generación se tienen que dar de baja y todos los volúmenes de agrupación de almacenamiento de tercera generación se tienen que actualizar a sólo lectura.

⁴ En una biblioteca con una unidad de sexta generación, es necesario dar de baja todos los volúmenes reutilizables de cuarta generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de cuarta generación a sólo lectura.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos LTO:

Tabla 2. Formato de grabación y capacidad estimada predeterminada para LTO

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.

Formato	Capacidad estimada	Descripción
ULTRIUM	100 GB	Formato sin comprimir, utilizando cartuchos Ultrium
ULTRIUMC	Consulte la nota 200 GB	Formato comprimido, utilizando cartuchos Ultrium
ULTRIUM2	200 GB	Formato sin comprimir (estándar) con cartuchos Ultrium 2
ULTRIUM2C	Consulte la nota 400 GB	Formato comprimido con cartuchos Ultrium 2
ULTRIUM3	400 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 3
ULTRIUM3C	Consulte la nota 800 GB	Formato comprimido, con cartuchos Ultrium 3
ULTRIUM4	800 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 4
ULTRIUM4C	Consulte la nota 1,6 TB	Formato comprimido con cartuchos Ultrium 4
ULTRIUM5	1,5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 5
ULTRIUM5C	Consulte la nota 3.0 TB	Formato comprimido con cartuchos Ultrium 5
ULTRIUM6	2.5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 6
ULTRIUM6C	Consulte la nota 6.25 TB	Formato comprimido con cartuchos Ultrium 6

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información sobre capacidades estimadas, consulte Tabla 2.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB . CD2 . E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@, #, \$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir). El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

Restricción: Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

Nota: No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.)

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.



Ejemplo: definir una clase de dispositivo LTO


Definir una clase de dispositivo que se denomina LTOTAPE para una unidad LTO en una biblioteca denominada LTOLIB. El formato es ULTRIUM, el límite de montaje es 12, la retención de montaje es 5, el prefijo del volumen de cinta se denomina SMVOL y la capacidad estimada es 100 GB.

```
define devclass ltotape devtype=lto library=ltolib
format=ultrium mountlimit=12 mountretention=5
prefix=smvol estcapacity=100G
```

DEFINE DEVCLASS (Definir una clase de dispositivo NAS)

Utilice la clase de dispositivo NAS cuando realice operaciones con el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad de servidores de archivos de almacenamiento conectado a red (NAS). La clase de dispositivo es para las unidades a las que da soporte el servidor de archivos NAS para copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo NAS no admite las bibliotecas EXTERNAL ni Remote Storage Manager.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFINE DEVclass--nombre_clase_dispositivo--DEVType====-NAS-->
>--LIBRARY====-nombre_biblioteca--MOUNTRetention====-0----->
  .-MOUNTWait====-60----- .-MOUNTLimit====-DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-MOUNTWait====-minutos-' '-MOUNTLimit====-+DRIVES+-'
                                     +-número+
                                     '-0-----'
>--ESTCAPacity====-tamaño----->
  .-PREFIX====-ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-PREFIX====-+ADSM-----+'
    '-prefijo_volumen_cinta-'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

DEVType=NAS (Necesario)

Especifica que se asigna a la clase de dispositivo el tipo de dispositivo de almacenamiento conectado a red (NAS). El tipo de dispositivo NAS es para unidades conectadas a un servidor de archivos NAS y que este utiliza para hacer copia de seguridad de sistemas de archivos NAS.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta SCSI utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

MOUNTRetention=0 (Necesario)

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Cero (0) es el único valor admitido para clases de dispositivo con DEVType=NAS.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

ESTCAPacity (Obligatorio)

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

Ejemplo: definir una clase de dispositivo NAS

Definir una clase de dispositivo denominada NASTAPE para una unidad NAS en una biblioteca denominada NASLIB. El límite de montaje es DRIVES, la retención de montaje es 0, el prefijo del volumen de cinta se denomina SMVOL y la capacidad estimada es 200

GB.

```
define devclass nastape devtype=nas library=naslib
mountretention=0 mountlimit=drives
prefix=smvol estcapacity=200G
```

DEFINE DEVCLASS (Definir una clase de dispositivo REMOVABLEFILE)

Utilice la clase de dispositivo REMOVABLEFILE para los dispositivos de medios extraíbles que están conectados como sistemas de archivos locales y extraíbles.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary---nombre_biblioteca--DEVType---REMOVABLEfile---->
  .-MAXCAPacity---espacio_restante-.
>-----+----->
  '-MAXCAPacity---tamaño-----'
  .-MOUNTRetention---60----- .-MOUNTWait---60-----.
>-----+----->
  '-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
  .-MOUNTLimit---DRIVES-----.
>-----+-----><
  '-MOUNTLimit---+DRIVES+-'
                    +-numero-+
                    '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)



Especifica el nombre del objeto de biblioteca definido que contiene las unidades de medios extraíbles que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

DEVType=REMOVABLEfile (Necesario)

Especifica que se asigna el tipo de dispositivo REMOVABLEFILE a la clase de dispositivo. REMOVABLEFILE indica que los volúmenes de esta clase de dispositivo son archivos en medios locales extraíbles.

Los volúmenes de una clase de dispositivo con un tipo de dispositivo REMOVABLEFILE son volúmenes de acceso secuencial.



Utilice las herramientas del fabricante del dispositivo para dar formato (si es necesario) al medio y etiquetarlo. La etiqueta del medio debe cumplir las siguientes restricciones:

- La etiqueta no puede tener más de 11 caracteres.
- La etiqueta del volumen y el nombre del archivo que figura en el volumen deben coincidir con exactitud.
-  Sistemas operativos AIX  Sistemas operativos Windows El valor del parámetro MAXCAPACITY debe ser menor que la capacidad del medio.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes definidos en una agrupación de almacenamiento clasificada por esta clase de dispositivo. Este parámetro es opcional.

El parámetro MAXCAPACITY debe establecerse en un valor inferior a la capacidad del medio. Para los medios de CD, la capacidad máxima no debe exceder de 650 MB.

 Sistemas operativos AIX  Sistemas operativos Windows Dado que el servidor abre únicamente un archivo por medio físico extraíble, especifique una capacidad que permita que un archivo pueda utilizar totalmente la capacidad de su medio.

espacio_restante

La capacidad máxima predeterminada es el espacio que queda en el medio después de utilizarlo por primera vez.

tamaño

Debe especificar este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes).

Por ejemplo, MAXCAPACITY=5M especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 MB. El valor más pequeño permitido es 1 MB (es decir, MAXCAPACITY=1M).

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DEFINE DEVCLASS (Definir una clase de dispositivo SERVER)

Utilice la clase de dispositivo SERVER para utilizar los volúmenes de almacenamiento o los archivos archivados en otro servidor de IBM Spectrum Protect.

Si la protección de retención de datos se activa con el mandato SET ARCHIVERETENTIONPROTECTION, no podrá definir una clase de dispositivo de servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--DEVType-----SERVER--SERVERName-----nombre_servidor----->
  .-MAXCAPacity-----500M---.  .-MOUNTLimit-----1----->
>-----+-----+-----+-----+-----+----->
  '-MAXCAPacity-----tamaño-'  '-MOUNTLimit-----número-'
  .-MOUNTRetention-----60----->
>-----+-----+-----+-----+-----+----->
  '-MOUNTRetention-----minutos-'
  .-PREFIX-----ADSM----->
>-----+-----+-----+-----+-----+----->
  '-PREFIX-----ADSM-----+-'
      '-prefijo_volumen-'
  .-RETRYPeriod-----10----->
>-----+-----+-----+-----+-----+----->
  '-RETRYPeriod-----valor_reintento_(minutos)-'
  .-RETRYInterval-----30----->
>-----+-----+-----+-----+-----+----->>
  '-RETRYInterval-----retry_value_(seconds)-'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

DEVType=SERVER (Necesario)

Especifica una conexión remota que permite utilizar volúmenes virtuales.

SERVERName (Necesario)

Especifica el nombre del servidor. El parámetro SERVERNAME debe coincidir con un servidor definido.

MAXCAPacity

Especifica el tamaño máximo de los objetos creados en el servidor de destino; el valor predeterminado para este valor es 500M. Este parámetro es opcional.

500M

Especifica que la capacidad máxima es 500M (500 MB).

tamaño

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor mínimo permitido es 1 MB (MAXCAPACITY=1M).

MOUNTLimit

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino. Los intentos de acceder a más sesiones de las que indica el límite de montaje harán que el emisor de la solicitud tenga que esperar. Este parámetro es opcional. El valor predeterminado es 1. Puede especificar un número de 1 a 4096.

Los siguientes son los valores posibles:

1

Especifica que sólo se permite una sesión entre el servidor de origen y el servidor de destino.

número

Especifica el número de sesiones simultáneas entre el servidor de origen y el servidor de destino.

MOUNTRetention

Especifica el número de minutos que debe retenerse una conexión desocupada con el servidor de destino antes de que la conexión se cierre. Este parámetro es opcional. El valor predeterminado es 60. Puede especificar un número de 0 a 9999.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

RETRYPeriod

Especifica el período de reintento en minutos. El período de reintento es el intervalo de tiempo durante el cual el servidor debe intentar conectarse con un servidor destino, en caso de que se sospeche que existe un problema de comunicaciones. Este parámetro es opcional. Puede especificar un número de 0 a 9999. El valor predeterminado son 10 minutos.

RETRYInterval

Especifica el intervalo de reintentos en segundos. El intervalo de reintentos es la frecuencia con la que se realizan los intentos dentro de un período de tiempo específico. Este parámetro es opcional. Puede especificar un número de 1 a 9999. El valor predeterminado son 30 segundos.

DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE)

Utilice el tipo de dispositivo VOLSAFE para trabajar con medios y unidades de la marca StorageTek VolSafe. Esta tecnología utiliza medios que no se pueden sobregabar. Por consiguiente, no emplee estos medios para copias de seguridad a corto plazo de archivos de cliente, la base de datos de servidor o cintas de exportación.

Restricciones:

1. No se admiten las bibliotecas con conexión NAS.
2. Los medios VolSafe y los medios de lectura/grabación deben estar en agrupaciones de almacenamiento independientes.
3. Incorpore cartuchos CHECKLABEL=YES en el mandato CHECKIN LIBVOLUME.
4. Etiquete cartuchos con OVERWRITE=NO en el mandato LABEL LIBVOLUME. Si los cartuchos VolSafe se etiquetan más de una vez, no se podrán grabar datos adicionales en ellos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----VOLSAFE----->
>--WORM-----Yes--+-----+-----+-----+----->
      .-FORMAT----DRIVE-----+
      '-FORMAT----+DRIVE-----+'
          +-9840-----+
          +-9840-C----+
          +-T9840C----+
          +-T9840C-C--+
          +-T9840D----+
          +-T9840D-C--+
          +-T10000A---+
          +-T10000A-C-+
          +-T10000B---+
          +-T10000B-C-+
          +-T10000C---+
          +-T10000C-C-+
          +-T10000D---+
```


Formato	Capacidad estimada	Descripción
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS)

Utilice el mandato DEFINE DEVCLASS para definir una clase de dispositivo para un tipo de dispositivo de almacenamiento. El servidor exige que se defina una clase de dispositivo para poder utilizar un dispositivo. Hay disponible un conjunto limitado de tipos de clase de dispositivo para los dispositivos a los que se accede mediante un servidor de medios de z/OS.

- DEFINE DEVCLASS (Definir una clase de dispositivo 3590 para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS)

Tabla 1. Mandatos relacionados con DEFINE DEVCLASS

Mandato	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

DEVtype=3590 (Necesario)

Especifica que se asigna el tipo de dispositivo 3590 a la clase de dispositivo. 3590 indica que se asignan dispositivos de cartuchos de cinta IBM 3590 a esta clase de dispositivo.

Restricción: El servidor de medios de z/OS admite bloques de datos de 256 KB cuando la grabación se realiza en unidades de cinta 3590. Verifique que el hardware soporta esta posibilidad.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3590

Formato	Descripción
3590B	Formato sin comprimir (básico)
3590C	Formato comprimido
3590E-B	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Formato comprimido, similar al formato 3590C
3590H-B	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Formato comprimido, similar al formato 3590C

Nota: Si el formato utiliza la función de compresión por hardware de la unidad de cintas, la capacidad real puede disminuir, dependiendo de la eficacia de la compresión.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional. La capacidad estimada predeterminada para las cintas 3590 es de 9 GB.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: **K** (KB), **M** (MB), **G** (GB) o **T** (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADMS. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:
`AB.CD2.E`
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADMS.BFS.

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que dé soporte a la cinta 3590. Este parámetro es opcional. El nombre de unidad predeterminado es 3590. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS)

Para utilizar un servidor de medios de z/OS para acceder a los dispositivos 3592, debe definir una clase de dispositivo 3592. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY---biblioteca_medio_zos--DEVType----3592----->
.-FORMAT----Drive-----.-WORM----No-----.
```

```

>----->
'-FORMAT-----DRIVE-----' '-WORM-----Yes-+-'
      +-3592-----+
      +-3592C----+
      +-3592-2---+
      +-3592-2C--+
      +-3592-3---+
      +-3592-3C--+
      +-3592-4---+
      '-3592-4C-'

.-ESTCAPacity----300G---.
>----->
'-ESTCAPacity----tamaño-'

.-PREFIX----ADSM-----
>----->
'-PREFIX----ADSM-----'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention---60-----.-MOUNTWait---60-----.
>----->
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

.-MOUNTLimit---2-----.-COMPRESSION---Yes-----.
>----->
'-MOUNTLimit---+DRIVES-+-' '-COMPRESSION---+Yes-+-'
      +-número-+
      '-0-----'
      '-No--'

>----->
+EXPIration---yyyddd-+
'-RETention---días-----'

.-PROtection---No-----
>----->
'-PROtection---+No-----+'
      +-Yes-----+
      '-Automatic-'

.-UNIT----3592-----
>-----<
'-UNIT----nombre_unidad-'

```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

DEVTYPE=3592 (Necesario)

Especifica que se asigna el tipo de dispositivo 3592 a la clase de dispositivo.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3592

Formato	Descripción
3592	Formato sin comprimir (básico)
3592C	Formato comprimido
3592-2	Formato sin comprimir (básico), similar al formato 3592
3592-C	Formato comprimido, similar al formato 3592C

Formato	Descripción
3592-3	Formato sin comprimir (básico), similar al formato 3592
3592-3C	Formato comprimido, similar al formato 3592C
3592-4	Formato sin comprimir (básico), similar al formato 3592
3592-4C	Formato comprimido, similar al formato 3592C
DRIVE	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser distinta del valor que aparece en la lista.	

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades. Para un resultado óptimo, no mezcle las generaciones de unidades en la misma biblioteca. Si una biblioteca contiene una mezcla de generaciones, pueden darse problemas en los medios. Por ejemplo, las unidades de primera generación y segunda generación no pueden leer medios de tercera generación. Si es posible, actualice todas las unidades a 3592 de tercera generación. Si no puede actualizar todas las unidades a 3592 de tercera generación, debe utilizar una configuración especial.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Consejo: El servidor de IBM Spectrum Protect no suprime automáticamente volúmenes reutilizables en las agrupaciones de almacenamiento WORM después de que se vacíen los volúmenes por caducidad u otros procesos. Para suprimir estos volúmenes y eliminarlos de las agrupaciones de almacenamiento WORM, debe utilizar el mandato DELETE VOLUME. IBM Spectrum Protect no puede volver a utilizar volúmenes WORM grabados por el servidor y luego suprimidos de una agrupación de almacenamiento.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.

- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cintas que dé soporte a la cinta 3592. Este parámetro es opcional. El valor predeterminado es 3592. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)

Para utilizar un servidor de medios de z/OS para acceder a los dispositivos StorageTek como, por ejemplo, StorageTek T9840 o T10000, debe definir una clase de dispositivo ECARTRIDGE. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

Clase de privilegio

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. DRIVE es el valor predeterminado. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Nota:</p> <ul style="list-style-type: none"> Algunos formatos utilizan una función de compresión del hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista. Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C. 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional. La capacidad estimada predeterminada es de 9 GB.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que den soporte a las cintas ECARTRIDGE. Utilice el nombre de la unidad que representa el subconjunto de unidades de la biblioteca que están conectadas al sistema z/OS. Este parámetro es opcional. El valor predeterminado es 9840. El nombre de unidad puede tener hasta 8 caracteres.

Ejemplo: definir una clase de dispositivo con el tipo de dispositivo ECARTRIDGE

Defina una clase de dispositivo denominada E1 con el tipo de dispositivo ECARTRIDGE y con una protección RACF activa para todos los volúmenes de cinta asignados a esta clase de dispositivo. Para esta clase de dispositivo se comprimen todos los datos. La clase de dispositivo es para una biblioteca del servidor de medios de z/OS denominada ZOSELIB.

```
define devclass el devtype=ecartridge library=zoselib compression=yes
protection=yes
```

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS)

Para utilizar un servidor de medios de z/OS para acceder a los volúmenes de almacenamiento en los dispositivos de disco magnético, debe definir una clase de dispositivo FILE. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

Un volumen en esta clase de dispositivo es un conjunto de datos lineal VSAM (Virtual Storage Access Method) al que accede el servidor de medios de z/OS. Se pueden utilizar los volúmenes reutilizables con la clase de dispositivo y el servidor de medios de z/OS puede asignar dinámicamente el conjunto de datos lineal VSAM. No es necesario definir volúmenes para que el servidor utilice la clase de dispositivo. Si define volúmenes, establezca el calificador de alto nivel (HLQ) para que SMS reconozca la solicitud de asignación del servidor de medios de z/OS. Si utiliza volúmenes definidos, la función formatear volúmenes no se admite para el servidor al utilizar esta clase de dispositivo. El servidor de medios de z/OS utiliza una característica FormatWrite del gestor de medios DFSMS al llenar los volúmenes FILE.

Puede definir los volúmenes para la clase de dispositivo FILE utilizando el mandato DEFINE VOLUME. No obstante, el servidor de medios de z/OS no asigna espacio para un volumen definido hasta que se abra el volumen para su primer uso.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--DEVType----FILE--LIBRary----nombre_biblioteca----->
. -MAXCAPacity----10G----. . -PRIMARYalloc----2600M--.
>+-----+-----+-----+-----+-----+----->
' -MAXCAPacity----tamaño- ' ' -PRIMARYalloc----tamaño- '
. -SECONDARYalloc----2600M--.
>+-----+-----+-----+-----+-----+----->
' -SECONDARYalloc----tamaño- '
. -PREFIX----ADSM----- .
>+-----+-----+-----+-----+-----+----->
' -PREFIX----prefijo_volumen_archivo- '
. -MOUNTLimit----20----.
>+-----+-----+-----+-----+-----+-----><
' -MOUNTLimit----número- '
```

Parámetros

DEVType=FILE (Necesario)

Especifica que se asigna el tipo de dispositivo FILE a la clase de dispositivo.

LIBRary (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. servidor de medios de z/OS accede al almacenamiento de disco que utiliza esta clase de dispositivo y SMS controla dicho almacenamiento.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes de archivos definidos en una agrupación de almacenamiento de esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado son 10 GB (MAXCAPACITY=10G).

Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G).

PRIMARYALLOc

Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen. Debe haber disponible suficiente espacio para satisfacer la cantidad de asignación primaria. La política SMS (Storage Management Subsystem) determina si se pueden utilizar varios volúmenes físicos para satisfacer la petición de asignación primaria.

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 100 KB (PRIMARYALLOc=100K). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G). El tamaño predeterminado es 2600 MB (PRIMARYALLOc=2600M). Todos los valores se redondean al siguiente múltiple superior de 256 K.

Para evitar espacio desaprovechado, la operación de asignación dinámica utiliza el menor de los valores especificados en los dos parámetros PRIMARYALLOc y MAXCAPACITY.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOc y SECONDARYALLOc.

SECONDARYALLOc

Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado. El conjunto de datos de un volumen de archivos se amplía al tamaño establecido por el parámetro MAXCAPACITY y, a continuación, el volumen se marca como lleno.

Como la asignación secundaria de un conjunto de datos lineal no puede ocupar un volumen físico, tenga en cuenta el tamaño del volumen físico al seleccionar un tamaño de asignación secundaria. Por ejemplo, los volúmenes físicos de un modelo 3 de 3390 tienen aproximadamente 2,8 GB. Para garantizar que cada petición ocupe prácticamente un volumen físico completo, pero no más, utilice un tamaño de asignación secundario que sea un poco menor de 2,8 GB. Una cantidad de asignación secundaria de 2600 MB permite suficiente espacio para el conjunto de datos de volumen VSAM (VVDS), la etiqueta de volumen y la tabla de índice de volumen (VTOC).

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El valor mínimo es 0 KB (SECONDARYALLOc=0K). El valor predeterminado es 2600 MB. El valor máximo es 16384 GB. Excepto 0, todos los valores se redondean al siguiente múltiple superior de 256 K.

Si se especifica 0 (SECONDARYALLOc=0), el volumen de archivo no se puede ampliar más allá de la cantidad de asignación primaria.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOc y SECONDARYALLOc.

Si especifica un valor para el parámetro SECONDARYALLOCATION que no es 0, o si permite que el valor tome como valor predeterminado 2600M, la DATACLAS SMS asociada al identificador PREFIX (por ejemplo, calificador de alto nivel) debe tener especificado el atributo Extended Addressability (EA). Sin el atributo EA, la DATACLAS SMS limita la asignación del volumen FILE del conjunto de datos lineal VSAM a la ampliación primaria. (Consulte la descripción del parámetro PRIMARYALLOCATION). Con el conjunto de datos limitado al tamaño de asignación primario, el servidor de medios de z/OS no puede ampliar el conjunto de datos y el volumen se marca como FULL antes de que se alcance la capacidad máxima.

Restricción: Asegúrese de que los valores especificados para los parámetros PRIMARYALLOc y SECONDARYALLOc entren en los límites prácticos del dispositivo de almacenamiento. El servidor no puede comprobar si los valores exceden los límites prácticos del dispositivo y tampoco comprueba si los dos valores exceden conjuntamente el valor de MAXCAPACITY actual.

Consejo: Para rellenar los volúmenes cuando especifica un valor elevado para el parámetro MAXCAPACITY, especifique valores elevados para los parámetros PRIMARYALLOc y SECONDARYALLOc. Utilice tamaños de volumen de MVS mayores para reducir la posibilidad de anomalías de ampliación.

PREFIX

Especifica el calificador de nivel superior del nombre del conjunto de datos que se utiliza para asignar conjuntos de datos de volúmenes reutilizables. Para todos los volúmenes de archivos reutilizables creados en esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima del prefijo, incluidos los puntos, es de 32 caracteres.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB . CD2 . E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de conjunto de datos de volumen de archivo que utilice el prefijo predeterminado es
ADSM.B0000021.BFS.

Si tiene un convenio de denominación de conjunto de datos, utilice un prefijo que se ajuste a sus convenios de denominación. Por ejemplo, el siguiente valor es aceptable: TSM.SERVER2.VSAMFILE.

Si ejecuta varias instancias de servidor para IBM Spectrum Protect o Tivoli Storage Manager for z/OS Media, debe utilizar un valor exclusivo para el parámetro PREFIX en cada clase de dispositivo que defina.

MOUNTLimit

Especifica el número máximo de volúmenes FILE que se pueden abrir simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 20.

Si utiliza dispositivos IBM® 3995 que emulan dispositivos 3390, establezca el valor en un número menor que el número de corrientes de entrada y salida concurrentes que pueden existir en el medio físico.

El valor que especifique en este parámetro es importante si existe una importante penalización al conmutar de un volumen a otro. Por ejemplo, la conmutación puede llevarse a cabo cuando se utilizan dispositivos IBM 3995 que emulan dispositivos 3390. El valor que especifique no puede ser mayor que el número de unidades físicas disponibles en el dispositivo.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

DEFINE DOMAIN (Definir un nuevo dominio de políticas)

Utilice este mandato para definir un nuevo dominio de políticas. Un dominio de políticas contiene juegos de políticas, clases de gestión y grupos de copia. Se asigna un cliente a un dominio de políticas. El juego de políticas ACTIVE del dominio de políticas determina las reglas para los clientes asignados al dominio. Las reglas controlan los servicios de archivado, copia de seguridad y gestión de espacio proporcionados para los clientes.

Debe activar un juego de políticas del dominio para que los clientes asignados al dominio de políticas puedan ejecutar operaciones de copia de seguridad, archivado o migración de archivos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine Domain--nombre_dominio----->
>--+-----+----->
  '-DESCRiption---descripción-'
  .-BACKRETention---30---.  .-ARCHRETention---365--.
>--+-----+----->
  '-BACKRETention---días-'  '-ARCHRETention---días-'

>--+-----+----->>
  |                                     |
  |                                     v                                     |
  '-ACTIVEDESTination-----nombre_agrupación_datos_activos-----'
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

DESCRIPTION

Especifica una descripción del dominio de políticas. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

BACKRETention

Especifica el número de días (a partir de la fecha en que quedaron inactivas las versiones de copia de seguridad) que deben retenerse las versiones de copia de seguridad de los archivos que ya no están en el sistema de archivos del cliente. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 30. El servidor utiliza el valor de retención de copia de seguridad para gestionar las versiones inactivas de archivos cuando se producen cualquiera de las condiciones siguientes:

- Un archivo se vuelve a vincular a una nueva clase de gestión, pero ni la nueva clase de gestión ni la clase de gestión predeterminada contienen un grupo de copia de seguridad.
- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.

ARCHRETention

Especifica el número de días (desde la fecha de archivado) que se han de retener las copias archivadas. Este parámetro es opcional. Puede especificar un entero entre el 0 y el 30000. El valor predeterminado es 365. El servidor utiliza el valor de retención de copias archivadas para gestionar las copias archivadas cuando se produce una de las condiciones siguientes:

- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia archivada.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia archivada.

ACTIVEDESTination

Este parámetro opcional especifica los nombres de las agrupaciones de datos activos que almacenan versiones activas de datos de copias de seguridad para nodos asignados al dominio. Puede especificar hasta diez agrupaciones de datos activos para un dominio, separadas por comas. No se pueden utilizar espacios entre los nombres.

Antes de que el servidor de IBM Spectrum Protect grabe datos en una agrupación de datos activos, verifica si el nodo que posee los datos se ha asignado a un dominio que tiene la agrupación de datos activos que se indica en la lista ACTIVEDESTINATION. Si el servidor comprueba que el nodo cumple estos criterios, los datos se almacenarán en la agrupación de datos activos. Si el nodo no cumple los requisitos, los datos no se almacenarán en la agrupación de datos activos. Si la función de grabación simultánea se utiliza para grabar datos en una agrupación de datos activos, el servidor verifica que el nodo cumpla los criterios durante las operaciones de copia de seguridad de clientes de archivado y copia de seguridad de IBM Spectrum Protect o de clientes de aplicación mediante la API de IBM Spectrum Protect. La verificación también se realiza cuando se copian datos activos con el mandato COPY ACTIVE DATA.

Ejemplo: definir un dominio de políticas

Definir un dominio de políticas con el nombre PROG1 y la descripción Programming Group Domain. Se especificará que las copias archivadas deben retenerse 90 días cuando las clases de gestión o los grupos de copia archivada se suprimen y la clase de gestión predeterminada no contiene un grupo de copia archivada. También se especificará que las versiones de copia de seguridad deben retenerse 60 días cuando se suprimen las clases de gestión o los grupos de copia y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

```
define domain prog1
description="Programming Group Domain"
backretention=60 archretention=90
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE DOMAIN


Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

DEFINE DRIVE (Definir una unidad en una biblioteca)




Utilice este mandato para definir una unidad. Cada unidad se asigna a una biblioteca, por lo que debe definirse la biblioteca antes de emitir este mandato.

Después de haber emitido el mandato DEFINE DRIVE, debe especificarse una ruta con el fin de que IBM Spectrum Protect pueda utilizar la unidad. Para obtener más información, consulte el apartado DEFINE PATH (Definir una ruta). Si está utilizando un tipo de biblioteca SCSI o VTL, consulte PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca).

Puede definir más de una unidad para una biblioteca emitiendo el mandato DEFINE DRIVE para cada unidad. Las unidades autónomas siempre requieren una biblioteca manual.

 **Sistemas operativos Windows** Restricción: Antes de emitir el mandato DEFINE DRIVE para un dispositivo de medios extraíbles, como una unidad Jaz, Zip o de CD, deberá cargar en la unidad medios debidamente formateados y etiquetados.

Si quiere obtener información detallada y actual sobre el soporte de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  **Sistemas operativos AIX**  **Sistemas operativos Windows** Dispositivos compatibles con AIX y Windows
-  **Sistemas operativos Linux** Dispositivos compatibles con Linux

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine DRive--nombre_biblioteca--nombre_unidad----->
. -SERial-----AUTODetect----- . -ONLine-----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -SERial-----+--AUTODetect---+- ' ' -ONLine-----+--Yes+- '
      '-número_serie-'                '-No--'
                                     (1)
. -ELEment-----AUTODetect-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -ELEment-----+--AUTODetect+- '
      '-dirección--'

>+-----+-----+-----+-----+-----+-----+-----+-----+----->
|                                     (2) |
' -ACSDRVID-----id_unidad-----'

>+-----+-----+-----+-----+-----+-----+-----+-----+-----><
|                                     (3) |
' -CLEANFREQuency-----+--NONE-----+ '
      |                                     (4) |
      +--ASNEEDED-----+
      '-gigabytes-----'
```

Notas:

1. El parámetro ELEMENT sólo es necesario para unidades en bibliotecas SCSI cuando el tipo de unidad es una unidad NAS SCSI conectada a red.
2. Es necesario ACSDRVID para las unidades de las bibliotecas ACSLS. Este parámetro no es válido para las bibliotecas que no son ACSLS.
3. El parámetro CLEANFREQUENCY sólo es válido para unidades de las bibliotecas SCSI.
4. El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona para todas las unidades de cintas. Si desea obtener más información, consulte la descripción del parámetro.

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca a la que se asigna la unidad. Este parámetro es necesario para todas las unidades, incluidas las unidades autónomas. La biblioteca especificada deberá haberse definido anteriormente con el mandato DEFINE LIBRARY.

nombre_unidad (Obligatorio)

Especifica el nombre asignado a la unidad. La longitud máxima de este nombre es de 30 caracteres.

SERial

Especifica el número de serie de la unidad que se está definiendo. Este parámetro es opcional. El valor predeterminado es AUTODETECT.

Si SERIAL=AUTODETECT, el número de serie reportado por la unidad cuando defina la ruta se utiliza como el número de serie.

Si SERIAL=*número_serie*, el número de serie especificado se utiliza para verificar que la ruta de la unidad es correcta cuando se define la ruta.

Nota: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.

ONLine

Especifica si la unidad está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES.

Yes

Especifica que la unidad está disponible para utilizarla.

No

Especifica que la unidad no está disponible para utilizarla.

ELEMeNt

Especifica la dirección del elemento de una unidad dentro de una biblioteca de cintas virtual (VTL) o SCSI. El servidor utiliza la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI o VTL de la unidad. El valor predeterminado es AUTODETECT.

Si ELEMENT=AUTODETECT, cuando se defina la ruta de la unidad, el servidor detecta automáticamente el número de elemento.


Para localizar la dirección del elemento para la configuración de la biblioteca, consulte la información del fabricante.

Restricción:

- El parámetro ELEMENT solo es válido para unidades de bibliotecas SCSI o VTL cuando el tipo de unidad no es una unidad NAS (SCSI conectado a red).
- Este parámetro no es efectivo si se emite desde un servidor cliente de biblioteca (es decir, si el tipo de biblioteca es SHARED).
- En función de las posibilidades de la biblioteca, puede que ELEMENT=AUTODETECT no esté admitido. En este caso, debe proporcionar la dirección de elemento.

ACSDRVID

Especifica el ID de la unidad a la que se accede en una biblioteca SCSI. El identificador de unidad es un conjunto de números que indica la ubicación física de una unidad dentro de una biblioteca ACSLS. Este identificador de unidad debe especificarse como *a,l,p,d*, siendo *a* el ACSID, *l* el LSM (módulo de almacenamiento de biblioteca, *p* el número de panel y *d* el ID de unidad. El servidor necesita el identificador de unidad para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Consulte la documentación de StorageTek para obtener más detalles.

 Sistemas operativos Windows Restricción: Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

CLEANFREQuency

Especifica la frecuencia con que el servidor activa la limpieza de la unidad. Este parámetro es opcional. Para conseguir el grado de automatización de limpieza más completo para una biblioteca automatizada, deberá tener un cartucho limpiador que esté incorporado en el inventario de volúmenes de la biblioteca.

Si va a utilizar una limpieza basada en la biblioteca, se recomienda NONE cuando el tipo de biblioteca es compatible con esta función.

Este parámetro no es válido para las bibliotecas gestionadas externamente, por ejemplo las bibliotecas 3494 o las bibliotecas StorageTek que se gestionan bajo ACSLS.

Importante: Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades activada por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

NONE

Especifica que el servidor no hace el seguimiento de la limpieza de esta unidad. Puede utilizar este valor para las bibliotecas que tengan su propio sistema de limpieza automática.

ASNEEDED

Especifica que el servidor sólo carga la unidad con un cartucho limpiador dado de alta cuando una unidad notifica al controlador de dispositivo que es necesaria la limpieza.

El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo para ver información detallada de la unidad. Si ASNEEDED no está soportado, puede utilizar el valor gigabytes para la limpieza automática.

Con los controladores IBM 3592 e LTO, se recomienda la limpieza basada en la biblioteca. Si no se da soporte a la limpieza basada en la biblioteca, debe utilizarse ASNEEDED. Gigabytes no es recomendable.

Restricción: IBM Spectrum Protect no controla las unidades conectadas al servidor de archivos NAS. Si hay una unidad conectada sólo a un servidor de archivos NAS (no a un servidor o agente de almacenamiento), no especifique ASNEEDED como frecuencia de limpieza.

gigabytes

Especifica, en gigabytes, la cantidad de datos procesada en la unidad antes de que el servidor cargue la unidad con un cartucho limpiador. El servidor restablece el contador de gigabytes procesados cada vez que carga un cartucho limpiador en la unidad.

Importante: Cuando CLEANFREQUENCY=gigabyte, se puede producir la limpieza de unidad antes de que se alcance el valor de gigabytes, si la unidad notifica al controlador de dispositivo que es necesaria una limpieza.

Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si la información ofrece las recomendaciones para la frecuencia de limpieza en términos de horas de uso, convierta el valor en gigabytes realizando lo siguiente:

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor en gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.


Si se utiliza la frecuencia de limpieza recomendada por IBM® para las unidades de IBM, se garantiza que las unidades no se limpien más de lo necesario.

Para unidades IBM 3590, especifique un valor en gigabytes para la frecuencia de limpieza con el fin de garantizar que las unidades reciben la limpieza adecuada.

Ejemplo: definir una unidad en la biblioteca

Definir una unidad en una biblioteca manual con el nombre de biblioteca LIB01 y el nombre de unidad DRIVE01.

```
define drive lib01 drive01
```

 Sistemas operativos AIX

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/rmt0
```

 Sistemas operativos Linux

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/tmsmcsi/mt0
```


 Sistemas operativos Windows

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=mt3.0.0.0
```

Ejemplo: definir una unidad en una biblioteca ACSLS

Definir una unidad en una biblioteca ACSLS con un nombre de biblioteca de ACSLIB y un nombre de unidad de ACSDRV1 .

```
define drive acslib acsdrv1 acsdrv1=1,2,3,4
```

 Sistemas operativos AIX

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/rmt0
```

 Sistemas operativos Linux

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/tmsmcsi/mt0
```

 Sistemas operativos Windows

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=mt3.0.0.0
```

Ejemplo: definir una unidad en una biblioteca automática

Definir una unidad en una biblioteca automatizada cuyo nombre de biblioteca sea AUTO8MMLIB y el nombre de unidad DRIVE01.

```
define drive auto8mmlib drive01 element=82
```

Sistemas operativos AIX

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=/dev/rmt0
```

Sistemas operativos Linux

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=/dev/tmscsi/mt0
```

Sistemas operativos Windows

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=mt3.0.0.0
```

Mandos relacionados

Tabla 1. Mandatos relacionados con DEFINE DRIVE

Mandato	Descripción
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE PATH	Cambia los atributos asociados con una ruta.

DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)

Utilice este mandato para identificar un servidor como el servidor de eventos.

Si define un servidor de eventos, un servidor de IBM Spectrum Protect puede enviar eventos a otro servidor de IBM Spectrum Protect que anotará dichos eventos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine EVENTSErver--nombre_servidor-----><
```

Parámetros

nombre_servidor (Obligatorio)

Especifica el nombre del servidor de eventos. El servidor que especifique ya deberá haberse definido con el mandato DEFINE SERVER.

Ejemplo: designar el servidor de eventos

Designar ASTRO como el servidor de eventos.

```
define eventserver astro
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE EVENTSERVER

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE EVENTSERVER	Suprime la referencia a un servidor de eventos.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
PING SERVER	Prueba las conexiones entre servidores..
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.
QUERY SERVER	Muestra información sobre servidores.

Información relacionada:

[Anotaciones de eventos de empresa: anotaciones de eventos en otro servidor](#)

DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)

Utilice este mandato para agregar un servidor como miembro de un grupo de servidores. También se puede agregar un grupo de servidores a otro grupo de servidores. Un grupo de servidores permite direccionar mandatos a varios servidores especificando sólo el nombre del grupo de servidores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
      .- ,-----  
      v |  
>>-DEFine GRPMEMber--nombre_grupo----nombre_miembro-+----->>
```

Parámetros

nombre_grupo (Obligatorio)

Especifica el nombre del grupo de servidores al que se agregará el miembro.

nombre_miembro (Obligatorio)

Especifica los nombres de los servidores o grupos que se agregan al grupo. Para especificar varios servidores y grupos, debe separarlos con comas y sin espacios intercalados. Los servidores o grupos de servidores deben estar ya definidos en el servidor.

Ejemplo: definir un servidor para un grupo de servidores

Definir el servidor SANJOSE en el grupo de servidores CALIFORNIA.

```
define grpmember california sanjose
```

Ejemplo: definir un servidor y un grupo de servidores para un grupo de servidores

Definir el servidor TUCSON y el grupo de servidores CALIFORNIA en el grupo de servidores WEST_COMPLEX.

```
define grpmember west_complex tucson,california
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE GRPMEMBER

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.



Mandato	Descripción
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

DEFINE LIBRARY (Definir una biblioteca)




Utilice este mandato para definir una biblioteca. Una biblioteca es una colección de una o más unidades, y posiblemente dispositivos mecánicos, (dependiendo del tipo de biblioteca), los cuales se pueden utilizar para acceder a los volúmenes de almacenamiento.

A una biblioteca solo puede acceder un origen: un servidor de IBM Spectrum Protect o un transportador de datos. Sin embargo, las unidades de la biblioteca pueden accederse desde varios orígenes.

En el servidor pueden definirse los siguientes tipos de bibliotecas. Se proporcionan descripciones de sintaxis y parámetros para cada tipo.

- DEFINE LIBRARY (Definir una biblioteca 349X)
- DEFINE LIBRARY (Definir una biblioteca ACSLS)
- DEFINE LIBRARY (Definir una biblioteca externa)
- DEFINE LIBRARY (Definir una biblioteca FILE)
- DEFINE LIBRARY (Definir una biblioteca manual)
- DEFINE LIBRARY (Definir una biblioteca SCSI)
- DEFINE LIBRARY (Definir una biblioteca compartida)
- DEFINE LIBRARY (Definir una biblioteca VTL)
-  Sistemas operativos AIX  Sistemas operativos Linux **DEFINE LIBRARY (Definir un tipo de biblioteca ZOSMEDIA)**

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows **Dispositivos compatibles con AIX y Windows**
-  Sistemas operativos Linux **Dispositivos compatibles con Linux**

 **Sistemas operativos Windows**

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los mandatos DEFINE LIBRARY y UPDATE LIBRARY. Con este parámetro se evita tener que etiquetar previamente un conjunto de cintas. También es más eficaz que utilizar el mandato LABEL LIBVOLUME, para lo que es necesario montar los volúmenes por separado. Si utiliza el parámetro AUTOLABEL, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows porque IBM Spectrum Protect no proporciona programas de utilidad para formatear o etiquetar estos tipos de soporte. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el mandato label.

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE LIBRARY

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.

Mandato	Descripción
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE PATH	Cambia los atributos asociados con una ruta.

DEFINE LIBRARY (Definir una biblioteca 349X)

Utilice esta sintaxis para definir una biblioteca 349X.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType-----349X----->
. -SHARed-----No----- . -RESEtDrives-----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -SHARed-----+Yes-+- ' | (1) |
' -No-- ' ' -RESEtDrives-----+Yes-+- '
' -No-- '
. -AUTOLabel-----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel-----+No-----+ '
+Yes-----+
' -OVERWRITE- '
. -SCRATCHCAtegory-----301----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -SCRATCHCAtegory-----número- '
. -PRIVATECAtegory-----300----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -PRIVATECAtegory-----número- '
>+-----+-----+-----+-----+-----+-----+-----+-----><
' -WORMSCRatchcategory-----number- '
```

Notas:



1. El valor predeterminado para el parámetro RESETDRIVES es condicional. Si el parámetro SHARED está definido como NO, el valor del parámetro RESETDRIVES es NO. Si el parámetro SHARED está definido como YES, el valor del parámetro RESETDRIVES es YES.


Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=349X (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica que la biblioteca es un servidor de datos de biblioteca de cintas IBM 3494 ó 3495.

 Sistemas operativos Windows Especifica que la biblioteca es un servidor de datos de biblioteca de cintas IBM 3494 o un gestor de biblioteca de sistema de cintas IBM que emula un servidor de datos de biblioteca de cinta 3494.

Restricción: Las bibliotecas IBM 3494 solamente admiten un tipo de dispositivo exclusivo a la vez.

SHAREd

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHAREd=NO es necesario si la biblioteca se controla mediante mandatos pasados a través de un servidor de archivos NAS.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor sólo grabará encima de las etiquetas existentes si la etiqueta existente y también la etiqueta de código de barras todavía no se han definido en ninguna agrupación de almacenamiento del servidor o lista de histórico de volúmenes.

SCRATCHCAtegory

Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables en la biblioteca. Este parámetro es opcional. El valor predeterminado es 301 (se convierte en X'12D' en la biblioteca IBM 3494, pues ésta utiliza valores hexadecimales). Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca.

PRIVATECAtegory

Especifica el número de categoría para los volúmenes privados que deben montarse por nombre. Este parámetro es opcional. El valor predeterminado es 300 (este valor pasa a ser X'12C' en IBM 3494 porque utiliza valores hexadecimales). Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca.

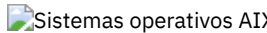

WORMSCRatchcategory


Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables WORM en la biblioteca. Este parámetro es necesario si utiliza volúmenes WORM. Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca. Este parámetro sólo es válido cuando se utilizan volúmenes WORM 3592.

Restricción: Si no se ha definido WORMSCRATCHCATEGORY y el parámetro WORM está establecido en YES para la clase de dispositivo, aparece un mensaje de error durante la operación de montaje.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

Ejemplo: definir una biblioteca 3494

Defina una biblioteca denominada `mi3494` con un número de categoría reutilizable 550, un número de categoría privado 600 y un número de categoría reutilizable de WORM igual a 400

```
define library my3494 libtype=349x scratchcategory=550
privatecategory=600 wormscratchcategory=400
```

DEFINE LIBRARY (Definir una biblioteca ACSLS)

Utilice esta sintaxis para definir una biblioteca ACSLS.

Clase de privilegio

 Sistemas operativos Windows Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType-----ACSLs----->
      .-SHARed-----No----- .-RESEtDrives-----No-----
>--+-----+-----+-----+-----+-----+-----+-----+----->
      '-SHARed-----+Yes+-' | (1) |
          '-No--'      '-RESEtDrives-----+Yes+-'
                          '-No--'

      .-AUTOLabel-----Yes-----
>--+-----+-----+-----+-----+-----+-----+-----+-----><
      '-AUTOLabel-----+No-----+
          +-Yes-----+
          '-OVERWRITE-'
```

Notas:

1. El valor predeterminado para el parámetro RESEtDRIVES es condicional. Si el parámetro SHARed está definido como NO, el valor del parámetro RESEtDRIVES es NO. Si el parámetro SHARed está definido como YES, el valor del parámetro RESEtDRIVES es YES.

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=ACSLs (Obligatorio)

Especifica que la biblioteca es una biblioteca StorageTek controlada mediante StorageTek ACSLS (Automated Cartridge System Library Software).

SHARed

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES



Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.


NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARed=NO es necesario si la biblioteca se controla mediante mandatos pasados a través de un servidor de archivos NAS.

RESEtDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de*

instalación y uso de los controladores de dispositivo de cinta de IBM.

- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

ACSID (Obligatorio)

Especifica el número de esta biblioteca StorageTek asignado por el ACSSA (Automatic Cartridge System System Administrator). Este un número puede ser del 0 al 126. Emita QUERY ACS en el sistema para obtener el número del identificador de la biblioteca. Este parámetro es necesario.

Para obtener más información, consulte la documentación de StorageTek.

Ejemplo: definir una biblioteca ACSLS compartida

Definir una biblioteca denominada ACSLIB con el tipo de biblioteca ACSLS y el ACSID 1.

```
define library acslib libtype=acsls acsid=1 shared=yes
```

DEFINE LIBRARY (Definir una biblioteca externa)

Utilice esta sintaxis para definir una biblioteca externa.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType----EXTernal----->
.-AUTOLabel----Yes-----
>--+-----+-----><
'-AUTOLabel----+-No-----+-'
      +-Yes-----+
      '-OVERWRITE-'
```



Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=EXTernal (Obligatorio)

Especifica que la biblioteca está gestionada con un sistema de gestión de medios externos. Este tipo de biblioteca no da soporte a las definiciones de unidades con el mandato DEFINE DRIVE. En su lugar, el sistema externo de gestión de medios identifica la unidad adecuada para las operaciones de acceso a los medios.

 Sistemas operativos AIX  Sistemas operativos Windows En un entorno IBM Spectrum Protect para redes de área de almacenamiento, este parámetro especifica que el software ACSLS (Automated Cartridge System Library Software) de StorageTek o el software de estación de biblioteca controla la biblioteca. Existe software, como Gresham EDT-DistribuTAPE, que permite que varios servidores puedan compartir la biblioteca. Las unidades de esta biblioteca no están definidas en IBM Spectrum Protect. ACSLS identifica la unidad para las operaciones de medios.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes




Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE




Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

Ejemplo: definir una biblioteca EXTERNAL para una configuración SAN

Para una configuración de IBM Spectrum Protect para redes de área de almacenamiento, definir una biblioteca denominada EXTLIB de tipo EXTERNAL. Si utiliza Gresham Enterprise DistribuTAPE, el archivo ejecutable del gestor de bibliotecas externo se encuentra en el directorio siguiente:

-  Sistemas operativos AIX/usr/lpp/dtelm/bin/elm
-  Sistemas operativos Linux/opt/OMIdtelm/bin/elm
-  Sistemas operativos Windowsc:\program files\GES\EDT\bin\elm.exe

Si va a utilizar IBM® Tape System Library Manager, el archivo ejecutable del gestor de bibliotecas externo se encuentra en el directorio siguiente:


-  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/TSLM/client/tsm/elm
-  Sistemas operativos Windows... \IBM\rmm\client\tsm\elm.exe

Para obtener más información, consulte la *IBM Tape System Library Manager User's Guide* en <http://www-01.ibm.com/support/docview.wss?uid=pub1ga32220802>.


1. Defina una biblioteca:

```
define library extlib libtype=external
```


2. Defina la ruta:

 Sistemas operativos AIX

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/usr/lpp/dtelm/bin/elm"
```

 Sistemas operativos Linux

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/opt/OMIdtelm/bin/elm"
```

 Sistemas operativos Windows

```
define path server1 extlib srctype=server desttype=library  
externalmanager="c:\program files\GES\EDT\bin\elm.exe"
```

DEFINE LIBRARY (Definir una biblioteca FILE)

Utilice esta sintaxis para definir una biblioteca FILE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRARY--nombre_biblioteca--LIBType-----FILE----->  
  
.-SHARED-----No-----.  
>--+-----+-----><  
'-SHARED-----+--Yes--+'  
      '-No--'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=FILE (Obligatorio)

Indica que se crea una pseudobiblioteca para volúmenes de archivos secuenciales. Cuando emite el mandato DEFINE DEVCLASS con los parámetros DEVTYPE=FILE y SHARED=YES, esto se produce automáticamente. Las bibliotecas FILE sólo son necesarias cuando se comparten volúmenes de archivos secuenciales entre el servidor y uno o más agentes de almacenamiento. Para utilizar las bibliotecas FILE es necesario el compartimento de bibliotecas. Las bibliotecas FILE compartidas se admiten para su uso en las configuraciones de copia de seguridad sin LAN solo. No puede utilizar una biblioteca FILE compartida en un entorno en el que se utiliza un gestor de biblioteca para gestionar los clientes de biblioteca.


SHARED

Especifica si esta biblioteca está compartida con otros servidores de IBM Spectrum Protect en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

NO

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

Ejemplo: definir una biblioteca manual

Definir una biblioteca denominada MANUALMOUNT con el tipo de biblioteca MANUAL.

```
define library manualmount libtype=manual
```

DEFINE LIBRARY (Definir una biblioteca SCSI)

Utilice esta sintaxis para definir una biblioteca SCSI.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType----SCSI----->
      .-SHARed----No----- .-RESEtDrives----No-----
>-+-----+-----+-----+-----+-----+-----+-----+----->
      '-SHARed----+-Yes-+-' | (1) |
          '-No--'      '-RESEtDrives----+-Yes-+-'
                          '-No--'

      .-AUTOLabel----No-----
>-+-----+-----+-----+-----+-----+-----+-----+----->
      '-AUTOLabel----+-No-----+-'
          +-Yes-----+
          '-OVERWRITE-'

      .-RELABELSCRatch----No-----.
```

```

>-----+----->
'-RELABELSCRatch-----+No--+-'
                          '-Yes-'

.-SERial-----AUTODetect-----
>-----+-----<<
'-SERial-----+AUTODetect-----+'
                          '-número_serie-'

```

Notas:

1. El valor predeterminado para el parámetro RESETDRIVES es condicional. Si el parámetro SHARED está definido como NO, el valor del parámetro RESETDRIVES es NO. Si el parámetro SHARED está definido como YES, el valor del parámetro RESETDRIVES es YES.

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=SCSI (Obligatorio)

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, el servidor utiliza el dispositivo cambiador de medios.

SHAREd

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHAREd=NO es necesario si la biblioteca se controla mediante mandatos pasados a través de un servidor de archivos NAS.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es NO.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes sólo si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando este parámetro se define con el valor SÍ, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta de volumen existente. Este parámetro es opcional y está pensado para utilizarse con una biblioteca de cintas virtual (VTL).

Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede influir en el rendimiento.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No



Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.


Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.
El dispositivo de biblioteca está conectado al dispositivo NAS, NDMP (protocolo de gestión de datos de red) accede indirectamente a él, y a las unidades de cintas solo se accede desde el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

SERial

Especifica el número de serie de la biblioteca que se está definiendo. Este parámetro es opcional. El valor predeterminado es AUTODETECT.

Si SERIAL=AUTODETECT, cuando defina la ruta a la biblioteca se utiliza como número de serie el indicado por la biblioteca.

Si SERIAL=*número_serie*, el número que ha entrado se compara con el número detectado por el servidor.




Atención: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.

Ejemplo: definir una biblioteca SCSI


Definir una biblioteca llamada SCسيلIB con un tipo de biblioteca de SCSI.

```
define library scsilib libtype=scsi
```


La biblioteca requiere una ruta. El nombre de dispositivo para la biblioteca es:

-  Sistemas operativos AIX/dev/lb0
-  Sistemas operativos Linux/dev/tmscsi/lb0
-  Sistemas operativos Windowslb3.0.0.0


Defina la ruta:

 Sistemas operativos AIX

```
define path server1 scsilib srctype=server desttype=library  
device=/dev/lb0
```

 Sistemas operativos Linux

```
define path server1 scsilib srctype=server desttype=library  
device=/dev/tmscsi/lb0
```

 Sistemas operativos Windows

```
define path server1 scsilib srctype=server desttype=library  
device=lb3.0.0.0
```

DEFINE LIBRARY (Definir una biblioteca compartida)

Utilice esta sintaxis para definir una biblioteca compartida.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRARY--nombre_biblioteca--LIBType-----SHARED----->  
>--PRIMarylibmanager--==--nombre_servidor-----><
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=SHARED (Obligatorio)

Especifica que la biblioteca está compartida con otro servidor de IBM Spectrum Protect por una red de área de almacenamiento (SAN) o una conexión SCSI dual con unidades de biblioteca.

Importante: Especifique este tipo de biblioteca cuando se defina la biblioteca en un cliente de bibliotecas.

PRIMarylibmanager

Especifica el nombre del servidor de IBM Spectrum Protect responsable del control del acceso a los recursos de biblioteca. Debe definir este servidor con el mandato DEFINE SERVER para poder utilizarlo como gestor de bibliotecas. Este parámetro sólo es necesario y válido si LIBTYPE=SHARED.

Ejemplo: definir una biblioteca compartida

En una SAN, defina una biblioteca denominada SHARED_{TSM} en un servidor de cliente de biblioteca denominado LIBMGR1


```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

DEFINE LIBRARY (Definir una biblioteca VTL)

Utilice esta sintaxis para definir una biblioteca que tenga un dispositivo cambiador de medios controlado por SCSI que se representa mediante una biblioteca de cintas virtual (VTL).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRARY--nombre_biblioteca--LIBType-----VTL----->
. -SHARED-----No----- . -RESETDrives-----No-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -SHARED-----+Yes--+ ' | (1) |
      '-No--'      '-RESETDrives-----+Yes--+-----'
                          '-No--'

. -AUTOLabel-----No-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel-----+No-----+-----+-----+-----+-----+-----+-----+----->
      +-Yes-----+
      '-OVERWRITE-'

. -RELABELSCRatch-----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -RELABELSCRatch-----+No--+-----+-----+-----+-----+-----+-----+----->
      '-Yes-'

. -SERial-----AUTODetect-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----><
' -SERial-----+AUTODetect-----+-----+-----+-----+-----+-----+-----+-----><
      '-número_serie-'
```

Notas:

1. El valor predeterminado para el parámetro RESETDRIVES es condicional. Si el parámetro SHARED está definido como NO, el valor del parámetro RESETDRIVES es NO. Si el parámetro SHARED está definido como YES, el valor del parámetro RESETDRIVES es YES.

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=VTL (Obligatorio)

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, el servidor utiliza el dispositivo cambiador de medios.

Si está definiendo una biblioteca VTL, el entorno no debe incluir ningún medio mixto y se deben definir rutas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento que utiliza la biblioteca. Si no se cumple alguna de estas características, el rendimiento general puede disminuir a los mismos niveles que el tipo de biblioteca SCSI; especialmente en momentos de gran actividad.

SHARED

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES



Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.


NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARED=NO es necesario si la biblioteca se controla mediante mandatos pasados a través de un servidor de archivos NAS.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es NO.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes sólo si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando se establece este parámetro en YES, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta del volumen existente.

Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede influir en el rendimiento.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar. YES es el valor predeterminado.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

SERIAL

Especifica el número de serie de la biblioteca que se está definiendo. Este parámetro es opcional. El valor predeterminado es AUTODETECT.

Si SERIAL=AUTODETECT, cuando defina la ruta a la biblioteca se utiliza como número de serie el indicado por la biblioteca.

Si SERIAL=*número_serie*, el número que ha entrado se compara con el número detectado por el servidor.




Atención: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.

Ejemplo: definir una biblioteca VTL


Definir una biblioteca denominada VTLLIB cuyo tipo de biblioteca sea VTL.

```
define library vtllib libtype=vtl
```

La biblioteca requiere una ruta. El nombre de dispositivo para la biblioteca es:

-  Sistemas operativos AIX/dev/lb0
-  Sistemas operativos Linux/dev/tmsmcsi/lb0
-  Sistemas operativos Windowslb3.0.0.0

Defina la ruta:

 Sistemas operativos AIX

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/lb0
```

 Sistemas operativos Linux

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/tmsmcsi/lb0
```

 Sistemas operativos Windows

```
define path server1 vtllib srctype=server desttype=library  
device=lb3.0.0.0
```

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE LIBRARY (Definir un tipo de biblioteca ZOSMEDIA)

Utilice esta sintaxis para definir una biblioteca que represente un recurso de almacenamiento TAPE o FILE mantenido por Tivoli Storage Manager for z/OS Media.

Defina una biblioteca de tipo ZOSMEDIA cuando desee que la biblioteca esté gestionada exclusivamente por Tivoli Storage Manager for z/OS Media. La biblioteca aparece para el servidor de IBM Spectrum Protect como un dispositivo de almacenamiento lógico que no requiere definiciones de DRIVE. Se necesita una definición de PATH para el servidor y los agentes de almacenamiento que necesitan acceso al recurso de biblioteca ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType-----ZOSMEDIA-----><
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir.

LIBType=ZOSMEDIA (Obligatorio)

Especifica que el tipo de biblioteca es ZOSMEDIA, que representa un recurso de almacenamiento TAPE o FILE mantenido por Tivoli Storage Manager for z/OS Media.

Ejemplo: configurar una biblioteca ZOSMEDIA

El siguiente ejemplo muestra los pasos necesarios para definir y configurar una biblioteca zosmedia. La configuración incluye estos componentes:

- Un servidor denominado sahara
- Una biblioteca definida como de tipo zosmedia denominada zebra
- Un servidor de medios de z/OS denominado oasis
- Un agente de almacenamiento denominado mirage

Defina una biblioteca denominada ZEBRA con un tipo de biblioteca ZOSMEDIA:

```
define library zebra libtype=zosmedia
```

Defina el servidor de medios de z/OS:

```
define server oasis serverpassword=sanddune  
hladdress=9.289.19.67 lladdress=1777
```

El servidor requiere una ruta al recurso de biblioteca gestionado por Tivoli Storage Manager for z/OS Media:

```
define path sahara zebra srctype=server  
desttype=library zosmediaserver=oasis
```

El agente de almacenamiento requiere una ruta al recurso de biblioteca gestionado por Tivoli Storage Manager for z/OS Media:

```
define path mirage zebra srctype=server  
desttype=library zosmediaserver=oasis
```

DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)

Utilice este mandato para guardar la información de recuperación ante siniestro para una máquina servidor o nodo cliente. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine MACHine--nombre_máquina----->  
  
>--+-----+--+-----+----->  
  '-DESCRiption----descripción-'  '-BUilding----edificio-'  
  
>--+-----+--+-----+----->  
  '-FLoor----planta-'  '-ROom----sala-'  
  
  .-PRIority----50-----  .-ADSMServer----No-----  
>--+-----+--+-----+----->  
  '-PRIority-----número--'  '-ADSMServer----+No---->
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina. El nombre puede estar formado por 64 caracteres como máximo.

DESCRiption

Especifica la descripción de una máquina. Este parámetro es opcional. El texto puede tener hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

BUilding

Especifica el edificio donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

FLOOR

Especifica la planta donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

ROom

Especifica la sala donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

PRIOriety

Especifica la prioridad de restauración de la máquina en forma de un entero del 1 al 99. La prioridad más alta es 1. Este parámetro es opcional. El valor predeterminado es 50.

ADSMServer

Especifica si la máquina es un servidor de IBM Spectrum Protect. Solo puede definirse una máquina como servidor de IBM Spectrum Protect. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Esta máquina no es un servidor de IBM Spectrum Protect.

Yes

Esta máquina es un servidor de IBM Spectrum Protect.

Ejemplo: definir la información de recuperación ante siniestro de una máquina

Definir una máquina denominada DISTRICT5 y especificar un nombre de ubicación, de planta y de sala. Esta máquina contiene datos esenciales y tiene la prioridad más alta.

```
define machine district5 building=101 floor=27
room=datafacilities priority=1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE MACHINE

Mandato	Descripción
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.
UPDATE MACHINE	Cambia la información para una máquina.

DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)

Utilice este mandato para asociar nodos cliente a una máquina. Durante la recuperación ante siniestro, puede utilizar esta información para identificar los nodos cliente que residían en las máquinas destruidas.

La máquina debe definirse y los nodos registrarse en IBM Spectrum Protect.

Para recuperar la información, emita el mandato QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Un nodo permanece asociado a una máquina mientras no se suprima el nodo, la máquina o la asociación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine MACHNODEAssociation--nombre_máquina----->
      .-,-----
      v          |
>----nombre_nodo+-----><
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina.

nombre_nodo (Obligatorio)

Especifica los nombres de nodo. Únicamente se puede asociar un nodo a una máquina. Para especificar varios nodos, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

Ejemplo: asociar un nodo a una máquina

Asociar el nodo denominado ACCOUNTSPAYABLE a la máquina denominada DISTRICT5.

```
define machnodeassociation district5 accountspayable
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE MACHNODEASSOCIATION

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
DELETE MACHNODEASSOCIATION	Suprime la asociación entre una máquina y un nodo.
QUERY MACHINE	Muestra información sobre máquinas.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.

DEFINE MGMTCLASS (Definir una clase de gestión)

Utilice este mandato para definir una nueva clase de gestión de un juego de políticas. Para que los clientes puedan utilizar la nueva clase de gestión, debe activar el juego de políticas que contiene la nueva clase.

Puede definir una o más clases de gestión para cada juego de políticas de un dominio de políticas. Una clase de gestión puede contener un grupo de copia de seguridad, un grupo de copia archivada, o ambos. El usuario de un nodo cliente puede seleccionar cualquier clase de gestión del juego de políticas activo o utilizar la clase de gestión predeterminada.

Atención: El mandato DEFINE MGMTCLASS no se ejecutará correctamente si se especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la clase de gestión.

Sintaxis

```
>>-DEFine MGmtclass--domain_name--policy_set_name--class_name-->
. -SPACEMGTEChnique-----NONE-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-SPACEMGTEChnique-----+--AUTOmatic-+-'
                                +-SElective-+
                                '-NONE-----'

. -AUTOMIGNOnuse-----0-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-AUTOMIGNOnuse-----días-'

. -MIGREQUIRESBkup-----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-MIGREQUIRESBkup-----+--Yes-+-'
                                '-No--'

. -MIGDESTination-----SPACEMGPOOL-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-MIGDESTination-----nombre_agrupación-'

>+-----+-----+-----+-----+-----+-----+-----+-----+-----><
  '-DESCRiption-----descripción-'
```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas al que pertenece la clase de gestión. No puede definir una clase de gestión en el juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica el nombre de la nueva clase de gestión. La longitud máxima de este nombre es de 30 caracteres. No puede utilizar *default* ni *grace_period* como nombre de clase.

SPACEMGTEChnique

Especifica si un archivo que utiliza esta clase de gestión se puede seleccionar para una operación de migración. Este parámetro es opcional. El valor predeterminado es NONE. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

AUTOmatic

Especifica que se puede seleccionar el archivo para la migración automática y para la migración selectiva.

SElective

Especifica que el archivo se puede seleccionar únicamente para la migración selectiva.

NONE

Especifica que el archivo no se puede seleccionar para la operación de migración.

AUTOMIGNOnuse

Especifica el número de días que deben transcurrir desde que se accedió por última vez a un archivo hasta que pueda seleccionarse para la migración automática. Este parámetro es opcional. El valor predeterminado es 0. Si SPACEMGTECHNIQUE no es AUTOMATIC, el servidor no tiene en cuenta este atributo. Puede especificar un entero en el rango 0 – 9999.

Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

MIGREQUIRESBkup

Especifica si debe existir una versión de copia de seguridad de un archivo antes de que pueda migrarse un archivo. Este parámetro es opcional. El valor predeterminado es YES. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

Yes

Especifica que debe existir una versión de copia de seguridad.

No

Especifica que la versión de copia de seguridad es opcional.

MIGDESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los archivos migrados mediante clientes de IBM Spectrum Protect for Space Management. Este parámetro sólo es efectivo para los clientes IBM Spectrum

Protect for Space Management, y no es efectivo para los clientes de copia de seguridad/archivado ni los clientes de aplicación. El valor predeterminado es SPACEMGPOOL.

La elección del destino puede depender de factores tales como los siguientes:

- El número de nodos cliente que se migran a la agrupación de almacenamiento. Cuando hay un gran número de archivos de usuario que se almacenan en la misma agrupación de almacenamiento, puede producirse la contención de volúmenes cuando los usuarios intentan migrar archivos a la agrupación de almacenamiento o recuperarlos de ésta.
- La velocidad con la que se deben recuperar los archivos. Si necesita acceso inmediato a las versiones migradas, puede especificar una agrupación de almacenamiento de disco como destino.

El mandato falla si especifica una agrupación de almacenamiento de copia o una agrupación de datos activos como destino.

DESCRiption

Especifica una descripción de la clase de gestión. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: definir una clase de gestión para un juego de políticas y un dominio de políticas específicos

Defina una clase de gestión que se denomina MCLASS1 para el conjunto de políticas SUMMER en el dominio de políticas PROG1. Para los clientes IBM Spectrum Protect for Space Management, se permitirá la migración automática y la migración selectiva, y los archivos migrados se almacenarán en la agrupación de almacenamiento SMPPOOL. Agregue la descripción, "Technical Support Mgmt Class."

```
define mgmtclass prog1 summer mclass1
spacemgtechnique=automatic migdestination=smpool
description="technical support mgmt class"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE MGMTCLASS

Mandato	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

DEFINE NODEGROUP (Definir un grupo de nodos)

Utilice este mandato para definir un grupo de nodos. Un *grupo de nodos* es un grupo de nodos cliente a los que se trata como si fuesen una única entidad. Un nodo puede ser un miembro de uno o más grupos de nodos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-DEFine NODEGroup--nombre_grupo----->
```



```
>--+-----+-----><
'-DESCRiption--==-descripci3n-'
```

Parámetros

nombre_grupo

Especifica el nombre del grupo de nodos que desea crear. La longitud máxima del nombre es de 64 caracteres. El nombre especificado podría no ser igual al de cualquier otro nombre de nodo de cliente existente.

DESCRiption

Especifica una descripción del grupo de nodos. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: definir un grupo de nodos

Definir un grupo de nodos denominado `group1`.

```
define nodegroup group1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE NODEGROUP

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)

Utilice este mandato para agregar un nodo cliente a un grupo de nodos. Un *grupo de nodos* es un grupo de nodos cliente a los que se trata como si fuesen una única entidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```

      .-+-----+
      v         |
>>-DEFine NODEGROUPMember--nombre_grupo----nombre_nodo-+-----><

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de nodos al que desea agregar un nodo cliente.

nombre_nodo

Especifica el nombre del nodo cliente que desea agregar al grupo de nodos. Puede especificar uno o más nombres. Separe varios nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín al especificar varios nodos.

Ejemplo: definir miembros de grupo de nodos

Definir dos miembros, `node1` y `node2`, para un grupo de nodos, `group1`.

```
define nodegroupmember group1 node1,node2
```

Mandatos relacionados




Tabla 1. Mandatos relacionados con DEFINE NODEGROUPMEMBER

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.






DEFINE PATH (Definir una ruta)

Utilice este mandato para definir una ruta para el acceso de un origen a un destino. Deben definirse un origen y un destino antes de definir una ruta. Por ejemplo, si se necesita una ruta entre un servidor y una unidad, primero deberá emitir el mandato DEFINE DRIVE y, a continuación, el mandato DEFINE PATH. Después de haber emitido el mandato DEFINE DRIVE, debe especificarse una ruta con el fin de que el servidor pueda utilizar la unidad.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de ruta.

- DEFINE PATH (Definir una ruta cuando el destino es una unidad)
- DEFINE PATH (Definir una ruta cuando el destino es una biblioteca)
-  Sistemas operativos AIX  Sistemas operativos Linux  DEFINE PATH (Definir una ruta cuando el destino es una biblioteca ZOSMEDIA)

Si quiere obtener información detallada y actual sobre soporte de dispositivos, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows  Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux  Dispositivos compatibles con Linux

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE PATH

Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.

Mandato	Descripción
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.
UPDATE PATH	Cambia los atributos asociados con una ruta.

DEFINE PATH (Definir una ruta cuando el destino es una unidad)

Utilice esta sintaxis cuando defina una ruta a una unidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine PATH--nombre_origen--nombre_destino----->
>--SRCType-----+--DATAMover--+-----+----->
      '-SERVer----'   '-AUTODetect-----+--No--+-'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY-----nombre_biblioteca----->
>----DEVIce-----+--nombre_dispositivo+----->
      '-FILE-----'
      .-GENERICTAPE-----No----- .-ONLine-----Yes-----
>--+-----+-----+-----+----->
      '-GENERICTAPE-----+--Yes+-'   '-ONLine-----+--Yes+-'
                          '-No--'      '-No--'
      .-DIRectory-----nombre_directorio_actual-.
>--+-----+-----+-----+-----><
      |           .-'-----'           |
      |           v           |         |
      '-DIRectory-----nombre_directorio+-----'
```

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

AUTODetect

Especifica si se actualiza automáticamente en la base de datos el número de serie de una unidad en el momento en que se defina la ruta. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente. El número de serie se sigue comparando con lo que ya hay en la base de datos correspondiente al dispositivo. El servidor emite un mensaje si existe una discrepancia.

Yes

Especifica que el número de serie no se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica al servidor.

Importante:

1. Si no ha establecido el número de serie al definir la unidad, el servidor siempre intenta detectar el número de serie, y AUTODETECT toma el valor YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. El uso de AUTODETECT=YES en este mandato significa que el número de serie establecido en la definición de unidad se actualiza con el número de serie detectado.
3. Si establece DESTTYPE=DRIVE y AUTODETECT=YES, el número de elemento de la unidad que se encuentra en la base de datos cambia automáticamente para reflejar el mismo número de elemento que corresponde al número de serie de esa unidad. Esto se aplica a las unidades de una biblioteca SCSI. Para obtener más información acerca del número de elemento, consulte DEFINE DRIVE.
4. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

DESTType=DRive (Obligatorio)

Especifica que el destino es una unidad. Cuando el destino es una unidad, debe especificar un nombre de biblioteca.

LIBRARY

Especifica el nombre de la biblioteca a la que se asigna la unidad. La biblioteca debe estar ya definida en el servidor. Si la ruta es de un transportador de datos NAS a una biblioteca, la biblioteca debe tener el LIBTYPE establecido en SCSI, 349X o ACSLS.

DEVICE

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.





 Sistemas operativos AIX  Sistemas operativos Windows El origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos AIX /dev/mt3  Sistemas operativos Windows mt3
De un agente de almacenamiento (en un sistema Windows) a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM® System Storage Serie N: rst01




 Sistemas operativos Linux El origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	/dev/tmscsi/mt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	/dev/tmscsi/mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM System Storage Serie N: rst01


Importante:

-  Sistemas operativos AIX  Sistemas operativos Linux Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf.  Sistemas operativos Windows Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo c:\winnt\ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp,

conéctese con el servidor de archivos mediante Telnet y emita el mandato SYSCONFIG. Utilice este mandato para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```

Sistemas operativos Windows GENERICTAPE

 Sistemas operativos Windows Indica si la unidad de cintas que se va a utilizar es un tipo de clase de dispositivo GENERICTAPE. Si el dispositivo es una unidad de cintas y no recibe soporte de IBM Spectrum Protect, pero es compatible para el sistema operativo Windows, puede utilizarlo con el formato de cinta genérico. Para utilizar la unidad, especifique GENERICTAPE=Yes al definir una ruta a la unidad. El valor predeterminado es No. Los valores posibles son:

Yes

Indica que la unidad de cintas que se va a utilizar es un tipo de clase de dispositivo GENERICTAPE.

No

Indica que la unidad de cintas que se va a utilizar no es un tipo de clase de dispositivo GENERICTAPE.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Por ejemplo, si la ruta desde un transportador de datos a una unidad está en línea, pero el transportador de datos o la unidad está fuera de línea, no puede utilizar la ruta.

DIRectory

Especifique las ubicaciones en las que el agente de almacenamiento lee y graba los archivos que representan volúmenes de almacenamiento para la clase de dispositivo FILE asociada a la biblioteca FILE. El parámetro DIRECTORY también se utiliza para los dispositivos de tipo REMOVABLEFILE. Para los dispositivos REMOVABLEFILE, el parámetro DIRECTORY proporciona información para el servidor (no un agente de almacenamiento) junto con el parámetro DRIVE para describir acceso al dispositivo. Este parámetro es opcional.


Para una ruta desde un agente de almacenamiento a un dispositivo FILE, este parámetro sólo es válido cuando se cumplen *todas* las condiciones siguientes:

- El tipo de origen es SERVER (lo que significa que se ha definido como servidor un agente de almacenamiento en este servidor).
- El nombre de origen es el nombre del agente de almacenamiento y *no* del servidor.
- El destino es una unidad lógica que forma parte de una biblioteca FILE creada cuando se definió la clase de dispositivo.

Si ha especificado varios directorios para la clase de dispositivo asociada a la biblioteca FILE, debe especificar el mismo número de directorios para cada ruta de la biblioteca FILE. No cambie o mueva los directorios existentes en el servidor que está utilizando el agente de almacenamiento, para que la clase de dispositivo y la ruta permanezcan sincronizadas. Está permitido agregar directorios. Si se especifica un número no coincidente de directorios, se puede producir una anomalía de tiempo de ejecución.

El valor predeterminado de DIRECTORY es el directorio del servidor en el momento en que se emite el mandato. El registro de Windows se utiliza para ubicar el valor predeterminado.

Utilice un convenio de denominación que le permita asociar el directorio a una unidad física determinada. Esto ayuda a garantizar que la configuración es válida para compartir la biblioteca FILE entre el servidor y el agente de almacenamiento. Si el agente de almacenamiento se encuentra en un sistema Windows, utilice un nombre del convenio de denominación universal (UNC). Cuando el agente de almacenamiento no dispone de permiso para acceder al almacenamiento remoto, experimenta anomalías de montaje.

 Sistemas operativos Windows La cuenta asociada con el servicio del agente de almacenamiento debe ser una cuenta del grupo de administradores local o una cuenta del grupo de administradores del dominio. Si la cuenta está en el grupo de administradores local, el identificador de usuario y la contraseña deben corresponderse con los de la cuenta con autorización para acceder al almacenamiento, tal como fueron proporcionados por el sistema que administra los elementos compartidos remotos. Por ejemplo, si un servidor SAMBA proporciona acceso al almacenamiento remoto, el identificador de usuario y la contraseña de la configuración SAMBA deben coincidir con los del identificador de usuario y la contraseña del administrador local asociado al servicio del agente de almacenamiento.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path stal file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```

En el ejemplo anterior, el mandato DEFINE DEVCLASS establece el sistema de archivos compartidos en el directorio al que accede el servidor como D:\FILEDIR\DIR1. Sin embargo, el agente de almacenamiento utiliza un nombre UNC \\192.168.1.10\FILEDIR\DIR1. Esto implica que el sistema con la dirección TCP/IP 192.168.1.10 está compartiendo el mismo directorio, que utiliza FILEDIR como nombre compartido. Asimismo, el servicio de agente de almacenamiento tiene una cuenta que puede acceder a este almacenamiento. Puede acceder a éste porque está asociado a una cuenta local con el mismo identificador de usuario y contraseña que 192.168.1.10 o a una cuenta de dominio disponible tanto en el agente de almacenamiento como en 192.168.1.10. Si es adecuado para la instalación, puede sustituir 192.168.1.10 por un nombre simbólico como:

```
example.yourcompany.com
```

Atención:

1. Los agentes de almacenamiento acceden a los volúmenes FILE sustituyendo un nombre de directorio de un nombre de volumen por un nombre de directorio de un directorio de la lista proporcionada por el mandato DEFINE PATH. Los directorios especificados en este parámetro no están validados en el servidor.
2. IBM Spectrum Protect no crea recursos compartidos, permisos ni monta el sistema de archivos destino. Debe realizar estas acciones antes de iniciar el agente de almacenamiento.

Ejemplo: definir una ruta desde un servidor hasta una unidad


Definir una ruta de un servidor a una unidad. En este caso, el nombre de servidor es *NET1*, el nombre de unidad es *TAPEDRV6*, la biblioteca es *NETLIB* y el nombre de dispositivo es *mt4*. Establecer AUTODETECT en NO.

```
define path net1 tapedrv6 srctype=server autodetect=no desttype=drive
library=netlib device=mt4
```

Ejemplo: definir una ruta desde un servidor de transportador de datos hasta una unidad para la realización de la copia de seguridad y la restauración

Definir una ruta desde un transportador de datos, que es un servidor de archivos NAS, hasta la unidad que el servidor de archivos NAS utilizará para operaciones de copia de seguridad y restauración. En este ejemplo, el transportador de datos NAS es *NAS1*, el nombre de unidad es *TAPEDRV3*, la biblioteca es *NASLIB* y el nombre de dispositivo para la unidad es *rst01*.

```
define path nas1 tapedrv3 srctype=datamover desttype=drive library=naslib
device=rst01
```

 Sistemas operativos Linux

Ejemplo: definir una ruta desde un agente de almacenamiento hasta una unidad para la realización de la copia de seguridad y la restauración

Definir una ruta desde el agente de almacenamiento *SA1* hasta la unidad que el agente de almacenamiento utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, la biblioteca es *TSMLIB*, la unidad es *TAPEDRV4* y el nombre de dispositivo para la unidad es */dev/tmsmcsi/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
device=/dev/tmsmcsi/mt3
```

 Sistemas operativos AIX  Sistemas operativos Windows

Ejemplo: definir una ruta desde un agente de almacenamiento hasta una unidad para la realización de la copia de seguridad y la restauración

Definir una ruta desde el agente de almacenamiento *SA1* hasta la unidad que el agente de almacenamiento utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, la biblioteca es *TSMLIB*, la unidad es *TAPEDRV4* y el nombre de dispositivo para la unidad es */dev/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
device=/dev/mt3
```

 Sistemas operativos AIX  Sistemas operativos Windows

Ejemplo: definir una ruta para otorgar al agente de almacenamiento acceso al almacenamiento de disco compartido

Definir una ruta que otorgue al agente de almacenamiento acceso a los archivos del almacenamiento de disco compartido con el servidor. La unidad *FILE9* se define para la biblioteca *FILE1* del servidor. El agente de almacenamiento *SA1* accede a *FILE9*. En el agente de almacenamiento, estos datos se encuentran en el directorio `\\192.168.1.10\filedata`.


 Sistemas operativos AIX Los datos para *FILE9* residen en el servidor, en `/tsmdata/filedata`.

 Sistemas operativos Windows Los datos para *FILE9* residen en el servidor, en `d:\tsmdata\filedata`.

```
define path sa1 file9 srctype=server desttype=drive library=file1 device=file
  directory="\\192.168.1.10\filedata"
```

Ejemplo: configurar un agente de almacenamiento para que utilice una biblioteca FILE


El siguiente ejemplo muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:  Sistemas operativos Windows

- `c:\server`
- `d:\server`
- `e:\server`

 Sistemas operativos AIX  Sistemas operativos Linux


- `/opt/tivoli1`
- `/opt/tivoli2`
- `/opt/tivoli3`

1. Utilice el siguiente mandato para configurar una biblioteca FILE denominada *CLASSA* con una unidad denominada *CLASSA1* en *SERVER1*:  Sistemas operativos Windows

```
define devclass classa devtype=file
  directory="c:\server,d:\server,e:\server"
  shared=yes mountlimit=1
```

 Sistemas operativos AIX  Sistemas operativos Linux


```
define devclass classa devtype=file
  directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
  shared=yes mountlimit=1
```



2. Quiere que el agente de almacenamiento *STA1* pueda utilizar la biblioteca FILE, para poder definir la siguiente ruta para el agente de almacenamiento *STA1*:  Sistemas operativos Windows


```
define path sta1 classa1 srctype=server desttype=drive device=file
  directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
  \\192.168.1.10\e\server" library=classa
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
define path sta1 classa1 srctype=server desttype=drive device=file
  directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

 Sistemas operativos Windows En este caso, el agente de almacenamiento, *STA1*, sustituye el nombre de directorio `c:\server` por el nombre de directorio `\\192.168.1.10\c\server` para poder acceder a los volúmenes FILE que se encuentran en el directorio `c:\server` del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux En este caso, el agente de almacenamiento, *STA1*, sustituye el nombre de directorio `/opt/tivoli1` por el nombre de directorio `/opt/ibm1/` para poder acceder a los volúmenes FILE que se encuentran en el directorio `/opt/tivoli1` del servidor.

3.  Sistemas operativos Windows *SERVER1* crea el volumen de archivo `c:\server\file1.dsm`. Si cambia más adelante el primer directorio de la clase de dispositivo con el mandato siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

SERVER1 todavía puede acceder al volumen de archivo `c:\server\file1.dsm`, pero el agente de almacenamiento *STA1* no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de

directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

4. Si se crea el volumen de archivo /opt/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,  
/opt/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /opt/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

DEFINE PATH (Definir una ruta cuando el destino es una biblioteca)

Utilice esta sintaxis cuando defina una ruta a una biblioteca.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine PATH--nombre_origen--nombre_destino----->  
  
          (1)  
>--SRCType-----+--DATAMover-----+----->  
          '-SERVer-----'   '-AUTODetect-----+--No--+-'  
                                     '-Yes-'  
  
>--DESTType-----LIBRARY--+-DEVIce-----nombre_dispositivo---+----->  
          '-EXTERNALManager-----nombre_ruta-'  
  
          .-ONLine-----Yes-----.  
>--+-----+----->  
          '-ONLine-----+--Yes--+-'  
          '-No--'
```

Notas:

1. DATAMOVER sólo se aplica a dispositivos NAS.

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

Atención: Para definir una ruta de un transportador de datos NAS a una biblioteca, la biblioteca debe tener LIBTYPE establecido en SCSI, 349x o ACSLS.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

AUTODetect

Especifica si se actualizará automáticamente en la base de datos el número de serie de una unidad o biblioteca en el momento en que se defina la ruta. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad o a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente. El número de serie se sigue comparando con lo que ya hay en la base de datos correspondiente al dispositivo. El servidor emite un mensaje si existe una discrepancia.

Yes

Especifica que el número de serie se actualizará automáticamente para reflejar el mismo número de serie que la unidad reporta a IBM Spectrum Protect.

Importante:

1. Si no ha establecido el número de serie al definir la unidad o la biblioteca, el servidor siempre intenta detectar el número de serie, y AUTODETECT toma el valor YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. El uso de AUTODETECT=YES en este mandato significa que el número de serie establecido en la definición de unidad o biblioteca se actualiza con el número de serie detectado.
3. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

DESTType=LIBRARY (Obligatorio)

Especifica que el destino es una biblioteca. Este parámetro es necesario.

DEVICE

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.

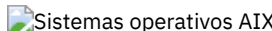
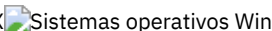



 Sistemas operativos AIX  Sistemas operativos Windows El origen utiliza el nombre de dispositivo para acceder a la biblioteca. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos AIX /dev/lb4  Sistemas operativos Linux /dev/tmsmcsi/lb4  Sistemas operativos Windows lb4.1
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una biblioteca	mc0

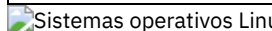

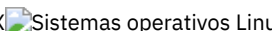

 Sistemas operativos Linux El origen utiliza el nombre de dispositivo para acceder a la biblioteca. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	/dev/tmsmcsi/lb4
De un transportador de datos NAS a una biblioteca	mc0

Importante:


-  Sistemas operativos AIX  Sistemas operativos Linux Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf.  Sistemas operativos Windows Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo c:\winnt\ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM® Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el mandato SYSCONFIG. Utilice este mandato para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```


Utilice este mandato para determinar el nombre de dispositivo para una biblioteca:

```
sysconfig -m
```


EXTERNALManager

Especifica la ubicación del gestor de bibliotecas externo donde IBM Spectrum Protect puede enviar peticiones de acceso a medio. Especifique el valor de este parámetro entre comillas simples. Por ejemplo, especifique:  Sistemas operativos AIX

/usr/lpp/GESedt-acsls/bin/elmdt

 Sistemas operativos Linux

/opt/GESedt-acsls/bin/elmdt

 Sistemas operativos Windows

C:\Archivos de programa\GES\EDT-ACSLs\bin\elmdt.exe

Este parámetro es necesario cuando el nombre de la biblioteca es una biblioteca externa.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.


No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Atención: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.

Ejemplo: definir una ruta desde un servidor hasta una biblioteca

Defina una ruta desde el servidor SATURN hacia la biblioteca de tipos SCSI SCSI LIB:  Sistemas operativos AIX

```
define path saturn scsilib srctype=server
desttype=library device=/dev/lb3
```

 Sistemas operativos Linux

```
define path saturn scsilib srctype=server
desttype=library device=/dev/tmscsi/lb3
```

 Sistemas operativos Windows

```
define path saturn scsilib srctype=server
desttype=library device=lb3.0.0.0
```

 Sistemas operativos AIX  Sistemas operativos Linux

DEFINE PATH (Definir una ruta cuando el destino es una biblioteca ZOSMEDIA)

Utilice esta sintaxis cuando defina una ruta a una biblioteca ZOSMEDIA. Debe definir el servidor de medios de z/OS en la configuración con el mandato DEFINE SERVER.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DEFine PATH--nombre_origen--nombre_destino----->
>--SRCType----SERVer--DESTType----LIBRary----->
                                     .-ONLine----Yes-----
>--ZOSMEDIASERVER----server_name--+-----+----->>
                                     '-ONLine----+Yes-+-'
                                     '-No--'
```

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta.

nombre_destino (Obligatorio)

Especifica el nombre de la biblioteca ZOSMEDIA.

SRCType=SERVer (Obligatorio)

Especifica que el origen es un servidor o un agente de almacenamiento.

DESTType=LIBRary (Obligatorio)

Especifica que el destino es una biblioteca.

ZOSMEDIAServer (Obligatorio)

Especifica el nombre del servidor que representa un servidor de Tivoli Storage Manager for z/OS Media.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Atención: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.

Si no se puede acceder a servidor de medios de z/OS durante la inicialización del servidor de IBM Spectrum Protect, se establecerá la ruta a la biblioteca en fuera de línea. Utilice el mandato UPDATE PATH y especifique ONLINE=YES para variar la biblioteca ZOSMEDIA de nuevo a en línea.

DEFINE POLICYSET (Definir un juego de políticas)

Utilice este mandato para definir un juego de políticas de un dominio de políticas. Un juego de políticas contiene clases de gestión, que contienen grupos de copia. Puede definir uno o varios juegos de políticas para cada dominio de políticas.

Para que un juego de políticas entre en vigor, debe activar el juego de políticas con el mandato ACTIVATE POLICYSET. Sólo puede haber un juego de políticas activo en un dominio de políticas. Los grupos de copia y las clases de gestión del juego de políticas activo determinan las reglas que siguen los nodos cliente para realizar las operaciones de copia de seguridad, archivado y gestión de espacio, y el modo en que se gestionan los archivos de cliente.

Utilice el mandato VALIDATE POLICYSET para verificar que un juego de políticas está completo y es válido antes de activarlo con el mandato ACTIVATE POLICYSET.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-DEFine Policyset--nombre_dominio--nombre_juego_políticas----->
>--+-----+-----+-----<
  '-DESCRiption--==-descripción-'
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del juego de políticas al que pertenece el juego de políticas.

nombre_juego_políticas (Necesario)

Especifica el nombre del juego de políticas. La longitud máxima de este nombre es de 30 caracteres. No puede definir un juego de políticas denominado ACTIVE.

DESCRiption

Especifica la descripción del nuevo juego de políticas. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: definir un juego de políticas

Definir un juego de políticas denominado `SUMMER` para el dominio de políticas `PROG1` e incluir la descripción, "Programming Group Policies".

```
define policyset prog1 summer
description="Programming Group Policies"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

DEFINE PROFASSOCIATION (Definir una asociación de perfil)

Utilice este mandato en un gestor de configuración para asociar uno o varios objetos con un perfil de configuración para distribuirlos a los servidores gestionados suscritos. Cuando un servidor gestionado se suscribe a un perfil, el gestor de configuración envía las definiciones de objeto asociadas con el perfil al servidor gestionado donde están almacenadas en la base de datos. Los objetos que se crean de este modo en la base de datos de un servidor gestionado se convierten en objetos gestionados. Un objeto se puede asociar a varios perfiles.

Puede utilizar este mandato para definir un conjunto inicial de asociaciones de perfiles y para agregarlo a asociaciones existentes.

Puede asociar a un perfil los tipos de objetos siguientes:

- Registros y autorizaciones de administrador
- Dominios de políticas, que incluyen los juegos de políticas, las clases de gestión, los grupos de copia y las planificaciones de cliente de los dominios.
- Planificaciones de administración
- Scripts de mandatos de servidor
- Conjuntos de opciones de cliente
- Definiciones del servidor
- Definiciones de grupos de servidores

Consejo: El gestor de configuración no distribuye información de estado sobre un objeto a los servidores gestionados. Por ejemplo, información como el número de días que han transcurrido desde la última vez que el administrador accedió al servidor no se distribuye a los servidores gestionados. Este tipo de información se mantiene en las bases de datos de cada servidor gestionado.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine PROFASSOCIation--nombre_perfil----->
```

```

>----->
'-ADMins-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_admin+--'

>----->
'-DOfains-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_dominio+--'

>----->
'-ADScheds-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_planificación+--'

>----->
'-ScripTs-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_script+--'

>----->
'-CLOptsets-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_conjunto_opciones+--'

>----->
'-SERVers-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_servidor+--'

>-----<
'-SERVERGroups-----+*-----+-'
      | .-,-----+ |
      | V             | |
      '---nombre_grupo+--'

```

Parámetros

nombre_perfil (Obligatorio)

Especifica el nombre del perfil de configuración.

ADMins

Especifica los administradores que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los administradores que están registrados en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros administradores, éstos se distribuirán automáticamente mediante el perfil.

El gestor de configuración distribuye el nombre de administrador, la contraseña, la información de contacto y las autorizaciones de los administradores asociados con el perfil. El gestor de configuración no distribuye lo siguiente:

- El administrador denominado SERVER_CONSOLE, aunque utilice la definición de coincidencia con todos
- El estado bloqueado o desbloqueado de un administrador

Si el perfil ya tiene administradores asociados, será aplicable lo siguiente:

- Si especifica una lista de administradores y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si especifica una definición de coincidencia con todos y ya existe una lista de administradores, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de administradores y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro ADMINS=*

DOfains

Especifica los dominios de políticas que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los dominios que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros dominios, éstos se distribuirán automáticamente mediante el perfil.

El gestor de configuración distribuye información de dominio que incluye las definiciones de los dominios de políticas, los juegos de políticas, las clases de gestión, los grupos de copia y las planificaciones de cliente. El gestor de configuración no distribuye el juego de políticas ACTIVE. Los administradores de un servidor gestionado pueden activar cualquier juego de políticas de un dominio gestionado en un servidor gestionado.

Si el perfil ya tiene dominios asociados, será aplicable lo siguiente:

- Si especifica una lista de dominios y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de dominios, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de dominios y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para eliminar la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro DOMAINS=*

Importante: Las operaciones de cliente como, por ejemplo, copia de seguridad y copia archivada no se ejecutarán si no existen las agrupaciones destino. Por lo tanto, los servidores gestionados suscritos a este perfil deben tener definiciones para todas las agrupaciones de almacenamiento especificadas como destino en los dominios asociados. Utilice el mandato RENAME STGPOOL para cambiar el nombre de las agrupaciones de almacenamiento existentes de modo que coincidan con los nombres de destino distribuidos.

ADScheds

Especifica las planificaciones de administración que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todas las planificaciones de administración que están definidas en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otras planificaciones de administración, éstas se distribuirán automáticamente mediante el perfil.

Consejo: Las planificaciones de administración no están activas cuando las distribuye un gestor de configuración. Un administrador de un servidor gestionado debe activar todas las planificaciones para que puedan ejecutarse en ese servidor. Si el perfil ya tiene planificaciones de administración asociadas, será aplicable lo siguiente:

- Si especifica una lista de planificaciones de administración y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de planificaciones de administración, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de planificaciones de administración y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro ADSCHEDS=*

SCRipts

Especifica los scripts de mandatos que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los scripts que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros scripts, éstos se distribuirán automáticamente mediante el perfil.

Si el perfil ya tiene scripts asociados, será aplicable lo siguiente:

- Si especifica una lista de scripts y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de scripts, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de scripts y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro SCRIPTS=*

CLOptsets

Especifica los conjuntos de opciones de cliente que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los conjuntos de opciones de cliente que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros conjuntos de opciones de cliente, éstos se distribuirán automáticamente mediante el perfil.

Si el perfil ya tiene conjuntos de opciones de cliente asociados, será aplicable lo siguiente:

- Si especifica una lista de conjuntos de opciones de cliente y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de conjuntos de opciones de cliente, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de conjuntos de opciones de cliente y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para eliminar la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro CLOPSETS=*.

SERVerS

Especifica las definiciones de servidor que se van a asociar al perfil. Las definiciones se distribuyen en los servidores gestionados que se inscriben en este perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los servidores que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros servidores, éstos se distribuirán automáticamente mediante el perfil.

El gestor de configuración distribuye los siguientes atributos de servidor: el método de comunicaciones, la dirección IP, la dirección de puerto, la contraseña del servidor, el URL y la descripción. Las definiciones de servidor distribuidas siempre tienen el atributo ALLOWREPLACE establecido en YES en el servidor gestionado, independientemente del valor que tenga este parámetro en el gestor de configuración. En el servidor gestionado, puede utilizar el mandato UPDATE SERVER para establecer todos los demás atributos.

Si el perfil ya tiene servidores asociados, será aplicable lo siguiente:

- Si especifica una lista de servidores y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de servidores, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de servidores y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro SERVERS=*.

Importante:

1. Una definición de servidor en un servidor gestionado no se sustituye por una definición del gestor de configuración a menos que se haya permitido sustituir la definición del servidor gestionado. Para permitir la sustitución, en el servidor gestionado, actualice la definición del servidor con el mandato UPDATE SERVER con ALLOWREPLACE=YES.
2. Si un gestor de configuración distribuye una definición de servidor a un servidor gestionado y existe un grupo de servidores con el mismo nombre en el servidor gestionado, la definición de servidor distribuida sustituye la definición del grupo de servidores.

SERVERGroups

Especifica los grupos de servidores que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (*) solo, para especificar todos los grupos de servidores que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros grupos de servidores, éstos se distribuirán automáticamente mediante el perfil.

Consejo: Un gestor de configuración no distribuye una definición de grupo de servidores a un servidor gestionado si el servidor gestionado tiene un servidor definido con el mismo nombre que el grupo de servidores.

Si el perfil ya tiene grupos de servidores asociados, será aplicable lo siguiente:

- Si especifica una lista de grupos de servidores y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de grupos de servidores, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de grupos de servidores y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el mandato DELETE PROFASSOCIATION con el parámetro SERVERGROUPS=*.

Ejemplo: asociar un dominio específico a un perfil específico

Asociar un dominio denominado MARKETING con un perfil denominado DELTA.

```
define profassociation delta domains=marketing
```

Ejemplo: asociar todos los dominios a un perfil específico

Ya tiene una lista de dominios asociada al perfil denominado GAMMA. Ahora asocie todos los dominios definidos en el gestor de configuración con el perfil.

```
define profassociation gamma domains=*
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE PROFASSOCIATION

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

DEFINE PROFILE (Definir un perfil)

Utilice este mandato en un gestor de configuración para definir un perfil (un conjunto de información de configuración) que se podrá distribuir a los servidores gestionados.

Después de haber definido un perfil, puede utilizar el mandato DEFINE PROFASSOCIATION para especificar los objetos que han de distribuirse a los servidores gestionados mediante la suscripción al perfil.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine PROFIle--nombre_perfil----->
>--+-----+-----><
  '-DESCRiption----descripción-'
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el nombre del perfil. La longitud máxima del nombre es de 30 caracteres.

DESCRiption

Especifica la descripción del perfil. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Este parámetro es opcional.

Ejemplo: definir un nuevo perfil

Defina un perfil de nombre ALPHA con una descripción de "Centro de programación".

```
define profile alpha
description="Programming Center"
```


Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)

Utilice este mandato para asociar un medio de recuperación a una o varias máquinas. Una máquina se asocia al medio de recuperación para que la ubicación del medio de arranque y la lista de nombres de volúmenes esté disponible para recuperar la máquina. Para recuperar la información, emita el mandato QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Para asociar una máquina a un medio de recuperación, la máquina y el medio deben estar definidos en IBM Spectrum Protect. Una máquina permanece asociada al medio mientras no se suprime la asociación, el medio o la máquina.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine RECMEDMACHAssociation--nombre_medio----->
      .-,-----
      v          |
>----nombre_máquina-+-----><
```

Parámetros

nombre_soporte (Obligatorio)

Especifica el nombre del medio de recuperación al que se asociarán una o varias máquinas.

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina que se ha de asociar al medio de recuperación. Una máquina puede asociarse a varios medios de recuperación. Para especificar una lista de máquinas, separe los nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

Ejemplo: asociar máquinas a medios de recuperación

Asociar las máquinas DISTRICT1 y DISTRICT5 al medio de recuperación DIST5RM.

```
define recmedmachassociation dist5rm
district1,district5
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE RECMEDMACHASSOCIATION

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE MACHINE	Suprime una máquina.
DELETE RECMEDMACHASSOCIATION	Suprime la asociación entre un medio de recuperación y una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY MACHINE	Muestra información sobre máquinas.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

DEFINE RECOVERYMEDIA (Definir medio de recuperación)

Utilice este mandato para definir el medio necesario para recuperar una máquina. El mismo medio puede estar asociado a varias máquinas. Para que se visualice la información, utilice el mandato QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine RECOVERYMedia--nombre_medio----->
>+-----+-----+-----+-----+----->
|           .-,'-----'. |
|           v             | |
|'-VOLumenames-----nombre_volumen-+-'|
>+-----+-----+-----+-----+----->
|'-DESCRiption-----descripción-'|
|
|                                     .-Type-----Other-----|
>+-----+-----+-----+-----+----->
|'-LOcation-----ubicación-'  '-Type-----+Other-+-'|
|                                     '-BOot--'|
>+-----+-----+-----+-----+----->
|'-PROduct-----nombre_producto-'|
>+-----+-----+-----+-----+-----><
|'-PRODUCTInfo-----información_producto-'|
```

Parámetros

nombre_soporte (Obligatorio)

Especifica el nombre del medio de recuperación que se ha de definir. El nombre puede tener hasta 30 caracteres.

VOLumenames

Especifica los de nombres de volúmenes que contienen datos recuperables (por ejemplo, copias de imágenes del sistema operativo). Este parámetro es necesario si especifica el tipo de medio BOOT. Los nombres de volúmenes de medios de arranque deben especificarse en el orden en que se insertarán en la máquina al efectuar la recuperación. La longitud máxima de la lista de nombres de volúmenes es de 255 caracteres. La lista debe estar delimitada por comillas si contiene algún carácter en blanco.

DESCRIPTION

Especifica la descripción del medio de recuperación. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

LOCATION

Especifica la ubicación del medio de recuperación. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Type

Especifica el tipo de medio de recuperación. Este parámetro es opcional. El valor predeterminado es OTHER.

BOot

Especifica que este es un medio de arranque. Debe especificar los nombres de los volúmenes si el tipo es BOOT.

OTHer

Especifica que éste no es un medio de arranque. Por ejemplo, un CD que contiene los manuales del sistema operativo.

PRoDuct

Especifica el nombre del producto que se ha grabado en este medio. Este parámetro es opcional. La longitud máxima son 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

PRoDuctInfo

Especifica la información sobre el producto que se ha grabado en el medio. Esta información puede ser necesaria para restaurar la máquina. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Ejemplo: definir los medios necesarios para realizar la recuperación de una máquina

Definir el medio de recuperación denominado DIST5RM. Se incluirá la descripción y la ubicación.

```
define recoverymedia dist5rm
description="district 5 base system image"
location="district 1 vault"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE RECOVERYMEDIA

Mandato	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

DEFINE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)

Utilice este mandato para crear una planificación de cliente o de mandato de administración.

El mandato DEFINE SCHEDULE tiene dos formatos: uno si la planificación se aplica a las operaciones de cliente y el otro si la planificación se aplica a mandatos administrativos. En estos dos formatos, puede seleccionar las planificaciones de estilo clásico o mejorado. La sintaxis y los parámetros de cada formato se definen por separado.

Para cada planificación, se especifica un margen de puesta en marcha. El margen de puesta en marcha es el período de tiempo durante el cual debe iniciarse la planificación. La planificación no completará necesariamente el proceso dentro de este margen. Si el servidor no está ejecutándose cuando se arranca este margen, pero se arranca antes de que se alcance el final del margen definido, la planificación se ejecutará cuando se vuelva a arrancar el servidor. Las opciones asociadas a cada estilo de planificación (clásico y mejorado) determinan cuándo deben comenzar las ventanas de inicio de sesión.

Tabla 1. Mandatos relacionados con DEFINE SCHEDULE

Mandato	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY SCHEDULE	Muestra información sobre planificaciones.

Mandato	Descripción
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un mandato planificado.
SET MAXSCHEDESESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- DEFINE SCHEDULE (Definir una planificación de cliente)
Utilice el mandato DEFINE SCHEDULE para definir una planificación de cliente. IBM Spectrum Protect utiliza esta planificación para realizar automáticamente diversas operaciones de cliente para la estación de trabajo cliente en los intervalos o días especificados. Después de haber definido una planificación, utilice el mandato DEFINE ASSOCIATION para asociar el cliente a la planificación.
- DEFINE SCHEDULE (Definir una planificación para un mandato de administración)
Utilice el mandato DEFINE SCHEDULE para crear una nueva planificación para procesar un mandato de administración.

DEFINE SCHEDULE (Definir una planificación de cliente)

Utilice el mandato DEFINE SCHEDULE para definir una planificación de cliente. IBM Spectrum Protect utiliza esta planificación para realizar automáticamente diversas operaciones de cliente para la estación de trabajo cliente en los intervalos o días especificados. Después de haber definido una planificación, utilice el mandato DEFINE ASSOCIATION para asociar el cliente a la planificación.

Debe iniciar el planificador de cliente en la estación de trabajo cliente para que IBM Spectrum Protect procese la planificación.

No todos los clientes pueden ejecutar todas las operaciones planificadas, aunque pueda definir la planificación en el servidor y asociar ésta al cliente. Por ejemplo, un cliente Macintosh no puede ejecutar una planificación cuando la acción sea restaurar o recuperar archivos o ejecutar un script ejecutable. En los diferentes sistemas operativos cliente, un script ejecutable, también se conoce como un archivo de mandatos, un archivo por lotes o un script.

IBM Spectrum Protect no puede ejecutar varias planificaciones al mismo tiempo para el mismo nodo cliente.

Clase de privilegio

Para definir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado al dominio de políticas al que pertenece la planificación.

Sintaxis

Planificación de cliente clásica

```
>>-DEFine SCHedule--domain_name--schedule_name----->
>--+-----+-----+-----+-----+----->
  '-Type----Client-' '-DESCRiption----descripci3n-'

  .-ACTion----Incremental-----
>--+-----+-----+-----+-----+----->
  '-ACTion----+Incremental-----+'
      +-Selectiva-----+
      +-Archive--+-----+-----+-----+-----+
      |               |          .-"-----." |
      |               |          '-SUBACTion-----+' |
      |               |          '-FASTBack-' |
      +-Backup--+-----+-----+-----+-----+
      |               |          .-"-----." |
      |               |          '-SUBACTion-----+' |
      |               |          +-FASTBack----+ |
      |               |          +-SYSTEMState+ |
      |               |          +-VApp-----+ |
      |               |          '-VM-----' |
      +-REStore-----+-----+-----+-----+
      +-RETrieve-----+-----+-----+-----+
      +-IMAGEBACkup-----+-----+-----+-----+
      +-IMAGERESStore-----+-----+-----+-----+
```

```

+-Command-----+
+-Macro-----+
'-Deploy-----'

>-----+----->
'-Options-----serie_opción-'

                                     .-PRIority-----5-----.
>-----+-----+-----+-----+-----+----->
|          (1)          | '-PRIority-----número-'
'-OBJects-----serie_objeto-'

.-STARTDate-----fecha_actual-.
>-----+-----+----->
'-STARTDate-----fecha-----'

.-STARTTime-----hora_actual-. .-DURation-----1-----.
>-----+-----+-----+-----+----->
'-STARTTime-----hora-----' '-DURATION -----número-'

.-DURUnits-----Hours----- .-MAXRUNTime-----0-----.
>-----+-----+-----+-----+----->
'-DURUnits-----+Minutes-----' '-MAXRUNTime-----número-'
+Hours-----+
+Days-----+
'-INDefinite-'

.-SCHEDStyle-----Classic-. .-PERiod-----1-----.
>-----+-----+-----+-----+----->
'-SCHEDStyle-----Classic-' '-PERiod-----número-'

.-PERUnits-----Days-----
>-----+-----+-----+-----+----->
'-PERUnits-----+Hours-----+'
+Days-----+
+Weeks---+
+Months---+
+Years---+
'-Onetime-'

.-DAYofweek-----ANY-----
>-----+-----+-----+-----+----->
'-DAYofweek-----+ANY-----+'
+WEEKDay---+
+WEEKEnd---+
+Sunday---+
+Monday---+
+Tuesday---+
+Wednesday+
+Thursday--+
+Friday---+
'-SATurday--'

.-EXPIration-----Never-----
>-----+-----+-----+-----+-----><
'-EXPIration-----+Never--+-'
'-date--'

```

Notas:

1. El parámetro OBJECTS es opcional cuando ACTION=INCREMENTAL, pero es necesario para otras acciones.

Sintaxis

Planificación de cliente mejorada

```

>>-DEFine SCHEDule--domain_name--schedule_name----->
>-----+-----+-----+-----+----->
'-Type-----Client-' '-DESCRiption-----descripci3n-'

.-ACTIon-----Incremental-----
>-----+-----+-----+-----+----->
'-ACTIon-----+Incremental-----+'

```

```

+-Selectiva-----+
+-Archive-----+
|          '-SUBAction----FASTBack-'          |
+-Backup-----+
|          |          .-"-----."          |
|          |          '-SUBAction-----+'          |
|          |          +-FASTBack----+          |
|          |          +-SYSTEMState+          |
|          |          +-VApp-----+          |
|          |          '-VM-----+'          |
+-REStore-----+
+-RETRieve-----+
+-IMAGEBACKup-----+
+-IMAGERESStore-----+
+-Command-----+
'-Macro-----'

>-----+----->
'-OPTions----serie_opción-'

                                     .-PRIority----5-----.
>-----+-----+----->
|          (1)          |          '-PRIority----número-'
'-OBJects-----serie_objeto-'

.-STARTDate----fecha_actual-.
>-----+----->
'-STARTDate----fecha-----'

.-STARTTime----hora_actual-. .-DURation----1-----.
>-----+-----+----->
'-STARTTime----hora-----' '-DURation ----número-'

.-DURUnits----Hours----- .-MAXRUNtime----0-----.
>-----+-----+----->
'-DURUnits----+Minutes+-' '-MAXRUNtime----número-'
          +-Hours---+
          '-Days----'

                                     .-MONth----ANY----- .
>--SCHEDStyle----Enhanced-----+----->
          '-MONth----+ANY-----+'
                                     +-JANuary---+
                                     +-FebrUary---+
                                     +-MARch-----+
                                     +-APRil-----+
                                     +-May-----+
                                     +-JUNE-----+
                                     +-JULy-----+
                                     +-AUGust-----+
                                     +-September+
                                     +-October---+
                                     +-November--+
                                     '-December--'

.-DAYOFMonth----ANY----- .-WEEKofmonth----ANY----- .
>-----+-----+----->
'-DAYOFMonth----+ANY+-' '-WEEKofmonth----+ANY-----+'
          '-Day-'          +-First--+
          +-Second+
          +-Third--+
          +-FOurth+
          '-Last---'

.-DAYofweek----ANY----- .
>-----+-----+----->
'-DAYofweek----+ANY-----+'
          +-WEEKDay---+
          +-WEEKEnd---+
          +-SUNDay----+
          +-Monday----+
          +-TUESday---+
          +-WednesDay+
          +-THursday--+
          +-Friday----+
          '-SATurday--'

```


Especifica que se ha programado una copia de seguridad del estado del sistema.

VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

VM

Especifica que se ha programado una copia de seguridad VMware del cliente.

Deploy

Especifica si se actualizarán las estaciones de trabajo del cliente con paquetes de despliegue especificados con el parámetro OBJECTS. El parámetro OBJECTS debe contener dos especificaciones: los archivos del paquete que se deben recuperar y de dónde recuperarlos. Asegúrese de que los objetos están en orden *ubicación_archivos*. Por ejemplo:

```
define schedule standard deploy_1 action=DEPLOY objects=  
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\  
..\IBM_ANR_WIN"
```

Los valores de las siguientes opciones estarán restringidos si se especifica ACTION=DEPLOY:

PERUNITS

Especifique PERUNITS=ONETIME. Si especifica PERUNITS=PERIOD, el parámetro se omitirá.

DURUNITS

Especifique MINUTES, HOURS o DAYS para el parámetro DURUNITS. No especifique INDEFINITE.

SCHEDSTYLE

Especifique el estilo predeterminado, CLASSIC.


El mandato SCHEDULE falla si los parámetros no coinciden con los valores de parámetro necesarios, como V.R.M.F.

OPTions

Especifica las opciones que se especifican en el mandato planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el mandato planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de mandatos. Todas las opciones que se describen como válidas solamente en la línea de mandatos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el mandato planificado:


- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el mandato DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el mandato planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:
 - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Para especificar `domain all-local -c: -d:`, escriba:
 - `options='-domain="all-local -c: -d:"'`

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración

- Proceso de mandatos individuales desde el cliente de administración

OBJects

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando ACTION=INCREMENTAL. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un mandato o una macro, el objeto será el nombre del mandato o macro que debe ejecutarse.

Si especifica ACTION=INCREMENTAL sin especificar ningún valor para este parámetro, el mandato planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de
destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número
excesivo de argumentos de línea de
mandatos
```

Si especifica ACTION=ARCHIVE, INCREMENTAL o SELECTIVE para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.


Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofos. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofos. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar C:\ARCHIVO 2, D:\ARCHIVOS GIF y E:\ARCHIVO DE PRUEBA, escriba:
 - OBJECTS=' "C:\ARCHIVO 2" "D:\ARCHIVOS GIF" "E:\ARCHIVO DE PRUEBA" '
- Para especificar D:\ARCHIVO DE PRUEBA, escriba:
 - OBJECTS=' "D:\ARCHIVO DE PRUEBA" '
- Para especificar D:\PRUEBA,ARCHIVO:
 - OBJECTS=' " "D:\PRUEBA,ARCHIVO" " ' '

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar /home/archivo 2, /home/archivos gif y /home/archivo de prueba, escriba:
 - OBJECTS=' "/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba" '
- Para especificar /home/archivo de prueba, escriba:
 - OBJECTS=' "/home/archivo de prueba" '

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

Consejo: Defina las planificaciones con duraciones de más de 10 minutos. Con ello, el planificador de IBM Spectrum Protect dispondrá de tiempo suficiente para procesar la planificación y avisar al cliente.

DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

Minutes

Especifica que la duración del margen se define en minutos.

Hours

Especifica que la duración del margen se define en horas.

Days

Especifica que la duración del margen se define en días.

INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejo: El tiempo máximo de ejecución se calcula desde el principio de la ventana de inicio y no desde la hora en que se inician las sesiones en la ventana de inicio.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. El valor predeterminado es 0. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y no se emite ningún mensaje de aviso. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de una operación planificada son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todas las sesiones de cliente para esta operación deben finalizar a la 1:00 del mediodía. Si se siguen ejecutando una o varias sesiones después de la 1:00 del mediodía, el servidor emite un mensaje de aviso.

Consejo: También puede especificar un valor para *Alerta de tiempo de ejecución* de 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se puede ejecutar una planificación, o los días en los que se ejecuta. El valor predeterminado es la sintaxis clásica.

Los valores posibles son:

Classic

Los parámetros de la sintaxis Classic son: PERIOD, PERUNITS y DAYOFWEEK. No puede utilizar estos parámetros: MONTH, DAYOFMONTH y WEEKOFMONTH.

Enhanced

Los parámetros de la sintaxis Enhanced son: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No puede utilizar estos parámetros: PERIOD y PERUNITS.

PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

Days

Especifica que el período entre márgenes de puesta en marcha es en días.

Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUESday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

SATurday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada mes del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es el -1, el penúltimo es el -2, etc. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecuta una vez ese día.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecuta una vez durante esa semana.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

EXPIration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

Ejemplo: definir una planificación para una copia de seguridad incremental mensual

Definir una planificación denominada MONTHLY_BACKUP que inicia una copia de seguridad incremental de todos los nodos asociados. Especifique martes 1 de mayo de 2001 como fecha de inicio. Esta fecha no concuerda con el día de la semana especificado (domingo), por lo tanto el margen de puesta en marcha empieza en el primer domingo después del 1 de mayo de 2001 (05/01/2001). Los márgenes de puesta en marcha de esta planificación abarcan de las 01:00 a las 03:00. Esta planificación mensual inicia la copia de seguridad de los espacios de archivos c: y d: para todos los nodos asociados.

```
define schedule standard monthly_backup
description="Copia de seguridad mensual de las unidades c: y d:"
objects="c:\* d:\*"
startdate=05/01/2001 starttime=01:00
duration=2 durunits=hours period=1
perunits=months dayofweek=sunday
```

Ejemplo: definir una planificación para una copia de seguridad incremental semanal

Definir una planificación denominada WEEKLY_BACKUP que inicia una copia de seguridad incremental de todos los nodos asociados. El margen de puesta en marcha inicial para esta planificación abarca desde las 23:00:00 del sábado, 7 de junio de 1997 (07/06/1997), a las 03:00:00 del domingo, 8 de junio de 1997 (08/06/1997). Los márgenes siguientes comienzan a las 23:00:00, cada sábado. Cuando se ejecuta esta planificación, no se devuelve ningún mensaje al nodo cliente.

```
define schedule employee_records weekly_backup
startdate=06/07/1997 starttime=23:00 duration=4
durunits=hours perunits=weeks
dayofweek=saturday options=-quiet
```

Ejemplo: definir una planificación que archive un directorio específico trimestralmente

Actualizar una planificación de las copias específicas archivadas trimestralmente el último viernes del mes.

```
define schedule employee_records quarterly_archive
starttime=20:00 action=archive
object=/home/employee/records/*
duration=1 durunits=hour schedstyle=enhanced
month=mar,jun,sep,dec weekofmonth=last dayofweek=fri
```

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

Utilice el mandato DEFINE SCHEDULE para crear una nueva planificación para procesar un mandato de administración.

Puede incluir scripts en una planificación de mandato de administración para que se procesen automáticamente.

Nota:

1. No puede planificar el mandato MACRO ni el mandato QUERY ACTLOG.
2. Si va a planificar un mandato que especifique el parámetro WAIT, el parámetro debe establecerse en YES para que el proceso proporcione un código de retorno a la sesión que lo ha iniciado. Para obtener más información acerca del parámetro WAIT, consulte el apartado Proceso de mandatos de servidor.

Clase de privilegio

Para definir una planificación de mandatos de administración, debe tener privilegio de sistema.

Sintaxis

```
Planificación de administración clásica

>>-DEFine SChedule--nombre_planificación----->

>--+-----+---CMD---mandato----->
'-Type---Administrative-'

.-ACTIVE---No-.
>--+-----+-----+----->
'-ACTIVE---Yes-' '-DESCription---descripción-'

.-PRIority---5-----.-STARTDate---fecha_actual-.
>--+-----+-----+----->
'-PRIority---número-' '-STARTDate---fecha-----'

.-STARTTime---hora_actual-. .-DURation---1-----.
>--+-----+-----+----->
'-STARTTime---hora-----' '-DURation ---número-'

.-DURUnits---Hours-----.-MAXRUNtime---0-----.
>--+-----+-----+----->
'-DURUnits---+Minutes-----' '-MAXRUNtime---número-'
      +-Hours-----+
      +-Days-----+
      '-INDefinite-'

.-SCHEDStyle---Classic-. .-PERiod---1-----.
```

```

>--+-----+-----+-----+-----+----->
  '-SCHEDStyle---Classic-' '-PERiod---numero-'

  .-PERUnits---Days-----
>--+-----+-----+-----+-----+----->
  '-PERUnits---+Hours---+'
                    +-Days----+
                    +-Weeks---+
                    +-Months--+
                    +-Years---+
                    '-Onetime-'

  .-DAYofweek---ANY-----
>--+-----+-----+-----+-----+----->
  '-DAYofweek---+ANY---+'
                    +-WEEKDay---+
                    +-WEEKEnd---+
                    +-Sunday---+
                    +-Monday---+
                    +-Tuesday---+
                    +-Wednesday+
                    +-Thursday--+
                    +-Friday---+
                    '-Saturday--'

  .-EXPIration---Never-----
>--+-----+-----+-----+-----+-----<
  '-EXPIration---+Never---+'
                    '-date--'

```

Sintaxis

Planificación de administración mejorada

```

>>-DEFine SCHEDULE--nombre_planificación----->
>--+-----+-----+-----+-----+----->
  '-Type---Administrative-'

  .-ACTIVE---NO--
>--+-----+-----+-----+-----+----->
  '-ACTIVE---YES-' '-DESCRIPTION---descripción-'

  .-PRIority---5----- .-STARTDate---fecha_actual-
>--+-----+-----+-----+-----+----->
  '-PRIority---numero-' '-STARTDate---fecha-----'

  .-STARTTime---hora_actual- .-DURATION---1-----
>--+-----+-----+-----+-----+----->
  '-STARTTime---hora-----' '-DURATION ---numero-'

  .-DURUnits---Hours----- .-MAXRUNTime---0-----
>--+-----+-----+-----+-----+----->
  '-DURUnits---+Minutes---+' '-MAXRUNTime---numero-'
                    +-Hours---+
                    '-Days---'

                    .-MONTH---ANY-----
>--SCHEDStyle---Enhanced+-----+-----+----->
                    '-MONTH---+ANY---+'
                                +-January---+
                                +-February---+
                                +-MARCH-----+
                                +-APRil-----+
                                +-May-----+
                                +-JUNE-----+
                                +-JULy-----+
                                +-AUGust-----+
                                +-September---+
                                +-October---+
                                +-November---+
                                '-December--'

  .-DAYOFMonth---ANY----- .-WEEKofmonth---ANY-----

```

```

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DAYOFMonth--==--ANY--+' '-WEEKofmonth--==--ANY--+'
      '-Day-'                               +-First--+
                                           +-Second--+
                                           +-Third--+
                                           +-FOurth--+
                                           '-Last--+'

.-DAYofweek--==--ANY-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DAYofweek--==--ANY-----+'
      +-WEEKDay----+
      +-WEEKEnd----+
      +-SUNday----+
      +-Monday----+
      +-TUESday---+
      +-Wednesday--+
      +-THursday--+
      +-Friday-----+
      '-SATurday--+'

.-EXPIration--==--Never-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<
'-EXPIration--==--Never--+'
      '-date--+'

```

Parámetros

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de definir. Puede especificar hasta 30 caracteres para el nombre.

Type=Administrative

Especifica que se define una planificación para un mandato de administración. Este parámetro es opcional. Se presupone un mandato de administración si se especifica el parámetro CMD.

CMD (Obligatorio)

Especifica el mandato de administración que se planifica para procesarlo. La longitud máxima del nombre es de 512 caracteres. El mandato de administración debe estar delimitado por comillas si contiene algún carácter en blanco.

Restricción: No puede especificar caracteres de redirección con este parámetro.

ACTIVE

Especifica si IBM Spectrum Protect procesa una planificación de mandato de administración al producirse el margen de puesta en marcha. Este parámetro es opcional. El valor predeterminado es NO. La planificación de mandato de administración se debe establecer en estado activo con el mandato UPDATE SCHEDULE para que IBM Spectrum Protect pueda procesar la planificación. Los valores posibles son:

YES

Especifica que IBM Spectrum Protect procesa una planificación de mandato de administración al empezar el margen de puesta en marcha.

NO

Especifica que IBM Spectrum Protect no procesa una planificación de mandato de administración al empezar el margen de puesta en marcha.

DESCRiption

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

PRIOrity

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

Minutes

Especifica que la duración del margen se define en minutos.

Hours

Especifica que la duración del margen se define en horas.

Days

Especifica que la duración del margen se define en días.

INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales se deben completar los procesos del servidor que se han iniciado mediante los mandatos planificados. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejos:

- Es posible que los procesos no finalicen inmediatamente después de que los haya cancelado el planificador central. Finalizan cuando registran la notificación de cancelación del planificador central.
- El tiempo de ejecución máximo se calcula comenzando desde el momento en que se inicia el servidor. Si el mandato de planificación inicia más de un proceso, se calcula tiempo máximo de ejecución de cada proceso a partir del inicio del proceso.
- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.
- Este parámetro no se aplica si el mandato planificado no inicia un proceso de servidor.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. El valor predeterminado es 0. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y el planificador central no cancela procesos. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de un mandato planificado son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todos los procesos de servidor aplicables iniciados por el mandato se deben finalizar a la 1:00 del mediodía. Si uno o varios procesos aplicaciones continúan ejecutándose pasadas la 1:00 del mediodía, el planificador central cancela los procesos.

Consejo: También puede especificar como *hora de finalización* la 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se debe ejecutar una planificación, o los días en los que se debe ejecutar. El estilo puede ser clásica o mejorada. El valor predeterminado es la sintaxis clásica.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten para las planificaciones mejoradas los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS.

PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

Days

Especifica que el período entre márgenes de puesta en marcha es en días.

Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUesday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

SATurday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY. Esto significa que la planificación se ejecutará todos los meses del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es -1, el penúltimo es -2, etc. Puede especificar varios valores separados mediante comas, sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecutará una vez ese día.

El valor predeterminado es ANY. Esto significa que la planificación se ejecutará cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecutará una vez durante esa semana.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

EXPIration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

Ejemplo: definir una planificación para que se realice la copia de seguridad de la agrupación de almacenamiento primaria cada dos días

Definir una planificación denominada BACKUP_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. La copia de seguridad se ejecuta a las 8 p.m. cada dos días.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
active=yes starttime=20:00 period=2
```

Ejemplo: definir una planificación para que se realice la copia de seguridad de la agrupación de almacenamiento primaria dos veces al mes

Definir una planificación denominada BACKUP_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. Seleccionar una planificación mejorada y ejecutarla el día uno y el quince de cada mes.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
schedstyle=enhanced dayofmonth=1,15
```

DEFINE SCRATCHPADENTRY (Definir una entrada de registro)

Utilice este mandato para introducir datos en una línea nueva en el registro. La anotación es una tabla de base de datos que aloja el servidor. Puede utilizar el registro para almacenar información diversa en formato de tabla.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine SCRATCHPadentry--major_category--minor_category----->
>--subject--Line -===número--Data====datos-----><
```

Parámetros

major_category (obligatorio)

Especifica la categoría principal en la se almacenarán los datos. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

minor_category (obligatorio)

Especifica la categoría secundaria en la se almacenarán los datos. Las categorías secundarias son secciones dentro de categorías principales. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)

Especifica el tema bajo el que se almacenarán los datos. Los asuntos son secciones en categorías secundarias. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

Line (obligatorio)

Especifica el número de la línea en la que se almacenarán los datos. Las líneas son secciones dentro de los asuntos. Especifique un entero en el rango 1 – 1000.

Data (obligatorio)

Especifica los datos que se almacenarán en la línea. Puede entrar un máximo de 1000 caracteres. Ponga los datos entre comillas si los datos contienen uno o más espacios en blanco. Los datos distinguen entre mayúsculas y minúsculas.

Ejemplo: Definir una entrada de registro

Entre las fechas de vacaciones de un administrador, Jane, en una tabla que almacena información sobre la ubicación de todos los administradores.

```
define scratchpadentry admin_info location jane line=2 data=
"Fuera de la oficina del 1-15 Nov."
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SCRATCHPADENTRY

Mandato	Descripción
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.

Mandato	Descripción
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

DEFINE SCRIPT (definir un script de IBM Spectrum Protect)

Utilice este mandato para definir un script de IBM Spectrum Protect o para crear un nuevo script de IBM Spectrum Protect con el contenido de otro script.

La primera línea del script se puede definir con este mandato. Para agregar más líneas al script, utilice el mandato UPDATE SCRIPT.

Consejos:

- Si direcciona mandatos dentro de los scripts, delimite el servidor o el grupo de servidores con paréntesis y omita los dos puntos. De otro modo, si la sintaxis incluye el carácter de los dos puntos, el mandato no se redirecciona al emitirse el mandato RUN. En lugar de ello, el mandato sólo se ejecuta en el servidor desde el que se emite el mandato RUN.
- No puede redirigir la salida de un mandato desde un script de IBM Spectrum Protect. En su lugar, ejecute el script, y luego especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

Clase de privilegio

Para emitir este mandato, debe tener privilegio de operador, políticas, almacenamiento o sistema.

Sintaxis

```
>>-DEFine SCript--nombre_script----->
      .-Line-----001----.
>--+línea_mandatos--+-----+----->
  |      '-Line ---número-' |
  '-File-----nombre_archivo-----'
>+-----+-----<<
  '-DESCRiption-----descripción-'
```

Parámetros

nombre_script (Obligatorio)

Especifica el nombre del script que se va a definir. Puede especificar hasta 30 caracteres para el nombre.

línea_mandatos

Especifica el primer mandato de un script que se procesará. Debe especificar este parámetro (y el parámetro LINE de forma opcional) o el parámetro FILE.

El mandato que especifique puede contener variables de sustitución y se puede continuar en varias líneas si especifica un carácter de continuación (-) como último carácter del mandato. Las variables de sustitución se especifican con el carácter '\$', seguido de un número que indica el valor del parámetro al procesarse el script. Puede especificar hasta 1200 caracteres para la línea de mandatos. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco.

Puede ejecutar mandatos en serie, en paralelo o en serie y en paralelo, especificando los mandatos de script SERIAL o PARALLEL para el parámetro COMMAND_LINE . Puede ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente. Los mandatos se ejecutan en serie hasta que se encuentre un mandato en paralelo.

Pueden utilizarse sentencias de flujo lógico condicional. Estas sentencias incluyen IF, EXIT y GOTO.

Line

Especifica el número de línea de la línea de mandatos. Ya que los mandatos se especifican en varias líneas, los números de línea se utilizan para determinar el orden en que se procesan al ejecutar el script. La primera línea, o línea 001, es el valor predeterminado. Este parámetro es opcional.

File

Especifica el nombre del archivo cuyo contenido se lee en el script que se va a definir. El archivo debe residir en el servidor donde se ejecuta este mandato. Si especifica el parámetro FILE, no puede especificar una línea de mandatos ni un número de línea.

Puede crear un script consultando otro script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene al consultar el script se dirige al archivo que especifique con el parámetro OUTPUTFILE. Para crear el nuevo script, el contenido del script que se va a definir se leerá del archivo que especifique con el parámetro OUTPUTFILE.

DESCRIPCIÓN

Especifica la descripción del script. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Este parámetro es opcional.

Ejemplo: escribir un script para que se visualicen los clientes de AIX

Defina un script que muestre todos los clientes de AIX.

```
define script qaixc "select node_name from nodes
where platform_name='AIX'"
desc='Display aix clients'
```

Ejemplo: escribir y ejecutar un script para que se redireccione un mandato a un grupo de servidores

Defina y ejecute un script que direcciona el mandato QUERY STGPOOL a un grupo de servidores denominado DEV_GROUP.

```
define script qu_stg "(dev_group) query stgpool"

run qu_stg
```

Ejemplo: crear un script a partir de un script existente

Defina un script cuyas líneas de mandatos se lean de un archivo denominado MY.SCRIPT y especifique que el nuevo script se denomine AGADM. El archivo debe residir en el servidor y éste debe leerlo.

```
define script agadm file=my.script
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SCRIPT

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

Conceptos relacionados:

Uso de sentencias de flujo lógico en un script

Tareas relacionadas:

Definición de un script del servidor

Ejecución de mandatos en paralelo o en serie

Realización de tareas simultáneamente en varios servidores



Referencia relacionada:

Códigos de retorno de los scripts para IBM Spectrum Protect

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

Utilice este mandato para definir un servidor para utilizar funciones, tales como volúmenes virtuales, replicación de nodos, direccionamiento de mandatos y el movimiento de datos libre de la LAN, entre otros.

Utilice este mandato para definir un servidor para las funciones siguientes:

- Configuración de Enterprise
- Anotación de eventos Enterprise
- Direccionamiento de mandatos
- Volúmenes virtuales
- movimiento de datos sin LAN
- Réplica de nodo
-  Sistemas operativos AIX  Sistemas operativos Linux Movimiento de datos utilizando servidor de medios de z/OS
- Supervisión del estado de los servidores remotos
- Supervisión de alerta de los servidores remotos
- Exportación de servidor a servidor

Si utiliza un servidor de directorios LDAP para autenticar contraseñas, los servidores de destino deben estar configurados para las contraseñas autenticadas por LDAP. Los datos que se replican de un nodo que se autentica con un servidor de directorios LDAP son inaccesible si el servidor de réplica de destino no está configurado correctamente. Si el servidor de réplica de destino no está configurado, los datos replicados de un nodo LDAP todavía pueden seguir allí. Sin embargo, el servidor de réplica de destino debe estar configurado para que utilice LDAP si desea acceder a los datos.

El uso de volúmenes virtuales no está soportado si el servidor de origen y el servidor de destino residen en el mismo servidor de IBM Spectrum Protect.

Este mandato también se utiliza para definir un agente de almacenamiento de IBM Spectrum Protect como si fuese un servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

Para:



- Direccionamiento de mandatos
- Supervisión del estado de los servidores remotos
- Supervisión de alerta de los servidores remotos
- Exportación de servidor a servidor

Consejo: El direccionamiento de mandatos utiliza el ID y la contraseña del administrador que emite el mandato.

```
>>-DEFine--SERver--nombre_servidor--HLAddress-----ip_address---->
>--LLAddress-----puerto_tcp--+-----+----->
      '-COMMmethod-----TCP/IP-'
>--+-----+-----+-----+----->
      '-URL-----url-' '-DESCRiption-----descripción-'
      .-SSL-----No----- .
>--+-----+-----+-----+----->
      '-SSL-----+No--+-'
          '-Yes-'
      .-SESSIONSECurity----TRANSitional----- .
>--+-----+-----+-----+----->>
      '-SESSIONSECurity----+STRICT-----+-'
          '-TRANSitional-'
```

Sintaxis

Para:


- Configuración de Enterprise
- Anotación de eventos Enterprise
- Agente de almacenamiento
- Servidores de origen y destino de réplica de nodo
-  Sistemas operativos AIX  Sistemas operativos Linux servidor de medios de z/OS


```

>>-DEFine--SERver--nombre_servidor----->
>--SERVERPAssword-----contraseña--HLAddress-----ip_address----->
>--LLAddress-----puerto_tcp--+-----+----->
      '-COMMmethod-----TCPiP-'
>+-----+-----+-----+----->
      '-URL-----url-' '-DEScRiption-----descripción-'
      (1)
      .-CROSSDEFine-----No----- (2)
>+-----+-----+-----+----->
      '-CROSSDEFine-----+No--+-'
      '-Yes-'
      .-VALIdateprotocol-----No----- .-SSL-----No-----
>+-----+-----+-----+----->
      '-VALIdateprotocol-----+No--+-' '-SSL-----+No--+-'
      '-All-' '-Yes-'
      .-SESSiONSECurity-----TRANSiTional-----
>+-----+-----+-----+----->
      '-SESSiONSECurity-----+STRiCT-----+-'
      '-TRANSiTional-'
      .-TRANSFERMethod-----TcpiP-----
>+-----+-----+-----+----->
      '-TRANSFERMethod-----+TcpiP-----+-'
      | (3) |
      '-Fasp-----'

```

Notas:

1. El parámetro CROSSDEFINE no se aplica a las definiciones del agente de almacenamiento.
2. El parámetro VALIDATEPROTOCOL está en desuso y sólo se aplica a las definiciones del agente de almacenamiento.
3.  Sistemas operativos Linux El parámetro TRANSFERMETHOD solo está disponible en sistemas operativos Linux x86_64 .

Sintaxis correspondiente a volúmenes virtuales

```

>>-DEFine--SERver--nombre_servidor--PAssword-----contraseña----->
>--HLAddress-----ip_address--LLAddress-----puerto_tcp----->
>+-----+-----+-----+----->
      '-COMMmethod-----TCPiP-' '-URL-----url-'
>+-----+-----+-----+----->
      '-DELgraceperiod-----días-' '-NODEName-----nombre_nodo-'
      .-SSL-----No-----
>+-----+-----+-----+----->
      '-DEScRiption-----descripción-' '-SSL-----+No--+-'
      '-Yes-'
      .-SESSiONSECurity-----TRANSiTional-----
>+-----+-----+-----+----->
      '-SESSiONSECurity-----+STRiCT-----+-'
      '-TRANSiTional-'

```

Parámetros

nombre_servidor (Obligatorio)

Especifica el nombre del servidor. Este nombre debe ser exclusivo en el servidor. La longitud máxima de este nombre es de 64 caracteres.

Para la anotación de eventos de servidor a servidor, la compartición de bibliotecas y la réplica de nodo, debe especificar un nombre de servidor que coincida con el nombre que se ha establecido emitiendo el mandato SET SERVERNAME en el servidor de destino.

PAssword

Especifica la contraseña que se utiliza para iniciar la sesión en el servidor de destino para los volúmenes virtuales. Si especifica el parámetro NODENAME, también debe especificar el parámetro PASSWORD. Si especifica el parámetro PASSWORD pero no el parámetro NODENAME, el nombre de nodo toma de forma predeterminada el nombre de servidor especificado con el mandato SET SERVERNAME.

SERVERPAssword

Especifica la contraseña del servidor que se está definiendo. Esta contraseña debe coincidir con la que se ha establecido con el mandato SET SERVERPASSWORD. Este parámetro es necesario para las funciones de configuración empresarial y de registro de eventos de servidor a servidor.

HLAddress (Obligatorio)

Especifica la dirección IP (con formato de coma decimal) del servidor.

No utilice la dirección de bucle de retorno como valor para este parámetro. Los volúmenes virtuales no están permitidos si el servidor origen y el servidor destino residen en el mismo servidor de IBM Spectrum Protect.

LLAddress (Obligatorio)

Especifica la dirección de bajo nivel del servidor. Esta dirección suele coincidir con la dirección de la opción de servidor TCPPOINT del servidor destino. Cuando SSL=YES, el puerto ya debe estar designado para comunicaciones SSL en el servidor de destino.

COMMmethod

Especifica el método de comunicación que se utiliza para conectar con el servidor. Este parámetro es opcional.

URL

Especifica la dirección URL de este servidor. El parámetro es opcional.

DELgraceperiod

Especifica un número de días en que el objeto permanece en el servidor de destino después de haber sido marcado para suprimirlo. Puede especificar un valor de 0 a 9999. El valor predeterminado es 5. Este parámetro es opcional.

NODENAME

Especifica un nombre de nodo que ha de utilizar el servidor para conectarse con el servidor destino. Este parámetro es opcional. Si especifica el parámetro NODENAME, debe especificar también el parámetro PASSWORD. Si especifica el parámetro PASSWORD sin especificar el parámetro NODENAME, el nombre de nodo toma de forma predeterminada el nombre de servidor especificado con el mandato SET SERVERNAME.

DESCRiption

Especifica la descripción del servidor. El parámetro es opcional. La descripción puede tener hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

CROSSDEFine

Especifica si el servidor que ejecuta este mandato se define a sí mismo en el servidor que se especifica mediante este mandato. Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Importante: Este parámetro no se aplica a las definiciones del agente de almacenamiento.

Si se incluye este parámetro, también deberá emitir los mandatos SET SERVERNAME, SET SERVERPASSWORD, SET SERVERHLADDRESS, SET CROSSDEFINE y SET SERVERLLADDRESS. El valor predeterminado es NO.

Recuerde:

- Para las operaciones de réplica, los nombres de los servidores de réplica de origen y destino deben coincidir con los nombres especificados en este mandato.
- CROSSDEFINE puede utilizarse con SSL=YES si todas las condiciones especificadas para el parámetro SSL=YES existen en el servidor de origen y destino.

Puede especificar uno de los siguientes valores:

No

La definición cruzada no se ha completado.

Yes

La definición cruzada se ha completado.

VALIdateprotocol (en desuso)

Especifica una comprobación de redundancia cíclica para validar los datos enviados entre el agente de almacenamiento y el servidor de IBM Spectrum Protect. El parámetro es opcional. El valor predeterminado es NO.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2 y Tivoli Storage Manager Versión 7.1.8, la validación que se ha habilitado mediante este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

SSL

Especifica la modalidad de comunicación del servidor. El valor predeterminado es NO.

Importante: A partir de IBM Spectrum Protect V8.1.2 y Tivoli Storage Manager V7.1.8, el parámetro SSL utiliza SSL para cifrar ciertas comunicaciones con el servidor especificado, incluso si se especifica SSL=NO.

Las siguientes condiciones y consideraciones se aplican cuando especifica el parámetro SSL:

- Antes de iniciar los servidores, los certificados autofirmados de los servidores asociados deben estar en el archivo de base de datos de claves (cert.kdb) de cada uno de los servidores.
- Puede definir varios nombres de servidor con distintos parámetros en el mismo servidor de destino.
- Los agentes de almacenamiento puede emitir el mandato DSMSTA SETSTORAGESEVER e incluir los parámetros SSL para crear la base de datos clave.

Puede especificar uno de los siguientes valores:

No

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, excepto si el servidor envía o recibe datos de objeto. Los datos de objeto se envían y se reciben mediante TCP/IP. Si elige no cifrar los objetos de datos, el rendimiento del servidor será similar a la comunicación mediante una sesión TCP/IP y la sesión es segura.

Yes

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, incluso si el servidor envía o recibe datos de objeto.

SESSIONSECURITY

Especifica si el servidor que está definiendo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRICT

Especifica que se aplicarán los valores de seguridad más estrictos para el servidor que se define. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor especificado y un servidor IBM Spectrum Protect.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el servidor especificado pueda autenticarse en el servidor IBM Spectrum Protect:

- Tanto el servidor que se define como el servidor IBM Spectrum Protect deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el servidor que está definiendo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre él mismo y el servidor IBM Spectrum Protect.


Los servidores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en IBM Spectrum Protect.

TRANSITIONAL

Especifica que se aplican los valores de seguridad existentes para el servidor. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el servidor no cumplen nunca los requisitos para el valor STRICT, el servidor continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un servidor cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el servidor ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un servidor que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, el direccionamiento de mandatos o la exportación entre servidores, cuando un nodo o un administrador se autentica en el servidor IBM Spectrum Protect como nodo o administrador de otro servidor.

Sistemas operativos Linux TRANSFERMethod

 Sistemas operativos Linux Especifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN).

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP

puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, las operaciones de transferencia de datos fallan.

- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Si especifica TRANSFERMETHOD=FASP en el mandato PROTECT STGPOOL o REPLICATE NODE, ese valor altera temporalmente el parámetro TRANSFERMETHOD en los mandatos DEFINE SERVER y UPDATE SERVER.

Ejemplo: configurar dos servidores que utilicen SSL para comunicarse (configuración manual)

Consejo: Si ambos servidores están utilizando IBM Spectrum Protect V8.1.2 o un software posterior o el software de Tivoli Storage Manager V7.1.8, SSL se configura automáticamente entre los servidores y no se necesita configuración manual.

Si ninguno de los servidores está utilizando el software V8.1.2, V7.1.8, o posterior, debe configurar manualmente los dos servidores para utilizar SSL para comunicarse.

Las direcciones de servidor son las siguientes:

- ServerA está en `bfa.tucson.ibm.com`
- ServerB está en `bfb.tucson.ibm.com`

Complete los pasos siguientes para configurar los dos servidores para SSL:

1. Especifique la opción TCPPOPT 1500 para ambos servidores en el archivo de opciones `dsmserv.opt`.
2. Inicie los dos servidores.
3. Concluya los dos servidores para importar el certificado de socio `cert256`. Para ServerA, el certificado está en el directorio de instancia `/tsma`. Para ServerB, el certificado está en el directorio de instancia `/tsmb`.
4. Inicie los dos servidores. El archivo `/tsma/cert256.arm` se copia en `/tsmb/cert256.bfa.arm` en la dirección `bfb.tucson.ibm.com`. El archivo `/tsmb/cert256.arm` se copia en `/tsmb/cert256.bfb.arm` en la dirección `bfa.tucson.ibm.com`.
5. Emita el mandato siguiente:
 - Desde ServerA:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label "bfb" -file /tsma/cert256.bfb.arm
```

- En ServerB:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label "bfa" -file /tsmb/cert256.bfa.arm
```

En cada servidor, puede ver los certificados de la base de datos de claves con el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

6. Reinicie los servidores.
7. Consulte el mandato DEFINE SERVER. Para ServerA, emita el mandato de ejemplo siguiente:

```
DEFINE SERVER BFB hla=bfb.tucson.ibm.com lla=1542  
serverpa=passwordforbfb SSL=YES
```

Para ServerB, emita el mandato de ejemplo siguiente:

```
DEFINE SERVER BFA hla=bfa.tucson.ibm.com lla=1542  
serverpa=passwordforbfa SSL=YES
```

Si no utiliza SSL, emita el siguiente mandato de ejemplo DEFINE SERVER en ServerA:

```
DEFINE SERVER BFBTCP hla=bfb.tucson.ibm.com lla=1500  
serverpa=passwordforbfb SSL=NO
```

Si no utiliza SSL, emita el siguiente mandato de ejemplo DEFINE SERVER en ServerB:

```
DEFINE SERVER BFATCP hla=bfa.tucson.ibm.com lla=1500  
serverpa=passwordforbfa SSL=NO
```

Ejemplo: Definir un servidor para comunicarse con otro servidor utilizando la seguridad de sesión estricta.

Defina un nombre de servidor de SERVER1 para utilizar los parámetros de seguridad más estrictos para autenticarse con el servidor IBM Spectrum Protect.

```
define server server1 sessionsecurity=strict
```

Ejemplo: definir un servidor de destino

Un servidor destino tiene la dirección de alto nivel 9.116.2.67 y la dirección de bajo nivel 1570. Defina dicho servidor destino ante el servidor origen, denomínelo SERVER2 y establezca la contraseña en SECRET. Especifique que los objetos permanezcan en el servidor de destino durante siete días después de que se hayan marcado para la supresión.

```
define server server2 password=secret
    hladdress=9.115.3.45 lladdress=1570 delgraceperiod=7
```

Ejemplo: definir un servidor para que reciba mandatos de otros servidores

Definir un servidor que pueda recibir mandatos direccionados desde otros servidores. Denomine al servidor WEST_COMPLEX. Establezca la dirección de alto nivel en 9.172.12.35, la dirección de bajo nivel en 1500 y la dirección URL en http://west_complex:1580/.

```
define server west_complex
    hladdress=9.172.12.35 lladdress=1500
    url=http://west_complex:1580/
```

Ejemplo: establecer una definición cruzada para los dos servidores

Utilizar la definición cruzada para definir SERVER_A y SERVER_B.

1. En SERVER_B, especificar el nombre de servidor, la contraseña y las direcciones de alto y bajo nivel de SERVER_B. Especifica que se admite la definición cruzada.

```
set servername server_b
set serverpassword mylife
set serverhladdress 9.115.20.80
set serverlladdress 1860
set crossdefine on
```

2. En SERVER_A, especificar el nombre de servidor, la contraseña y las direcciones de alto y bajo nivel de SERVER_A.





```
set servername server_a
set serverpassword yourlife
set serverhladdress 9.115.20.97
set serverlladdress 1500
```

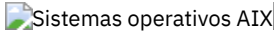
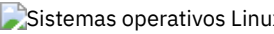
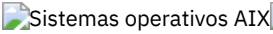
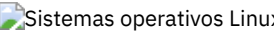
3. En SERVER_A, defina SERVER_B:

```
define server server_b hladdress=9.115.20.80 lladdress=1860
serverpassword=mylife crossdefine=yes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SERVER

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE PATH	 Sistemas operativos AIX  Sistemas operativos Linux Define una ruta cuando el destino es un servidor de medios de z/OS.
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.

Mandato	Descripción
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
  UPDATE PATH	  Define una ruta cuando el destino es un servidor de medios de z/OS.
UPDATE SERVER	Actualiza la información sobre un servidor.

DEFINE SERVERGROUP (Definir un grupo de nodo)

Utilice este mandato para definir un grupo de servidores. Con un grupo de servidores, puede direccionar mandatos a varios servidores especificando sólo el nombre del grupo. Después de haber definido el grupo de servidores, agregue servidores al grupo con el mandato DEFINE GRPMEMBER.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEfine SERVERGroup--nombre_grupo----->
>--+-----+-----><
  '-DEScRiption----descripción-'
```

Parámetros

nombre_grupo (Obligatorio)

Especifica el nombre del grupo de servidores. La longitud máxima del nombre es de 64 caracteres.

DEScRiption

Especifica una descripción del grupo de servidores. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: definir un grupo de servidores

Definir un grupo de servidores denominado WEST_COMPLEX.

```
define servergroup west_complex
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SERVERGROUP

Mandato	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.

Mandato	Descripción
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

DEFINE SPACETRIGGER (Definir desencadenante de espacio)

Utilice este mandato para definir los valores de los desencadenantes que determinan cuándo y cómo ha de preparar el servidor espacio adicional cuando se han excedido los umbrales predeterminados en las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE y DISK. Los desencadenantes de espacio no estarán activados para las agrupaciones de almacenamiento con un parámetro RECLAMATIONTYPE=SNAPLOCK.

El servidor IBM Spectrum Protect asigna más espacio cuando la utilización de espacio alcanza un valor especificado. Después de haber asignado espacio adicional, el servidor añade espacio a la agrupación especificada (disco de acceso aleatorio o de acceso secuencial).

Importante: Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Un cálculo no preciso puede dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar desactivado.

Por ejemplo, si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calculará el espacio añadiendo valores que representan el espacio que resta en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione el directorio que se ha especificado para la clase de dispositivo y que se produzca una condición de insuficiencia de espacio de forma prematura.

Para evitar posibles problemas y garantizar la obtención de un cálculo preciso, debe asociar cada directorio a un sistema de archivos distinto. Si un desencadenante se ha desactivado porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a activar el desencadenante especificando el mandato siguiente: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```

                                .-Fullpct----80----- .
>>-DEFine SPACETrigger---STG---+-----+----->
                                '-Fullpct----porcentaje-'

                                .-SPACEexpansion---20----- .
>--+-----+----->
                                '-SPACEexpansion---porcentaje-'

>--+-----+----->
                                '-EXPansionprefix---prefijo-'

>--+-----+-----<<
                                '-STGPOOL---nombre_agrupación_almacenamiento-'

```

Parámetros

STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

Fullpct

Este parámetro especifica el porcentaje de utilización de la agrupación de almacenamiento. Este parámetro es opcional. Especifique un valor entero de 0 a 99. El valor predeterminado es 80. Un valor de cero (0) inactiva el desencadenante de espacio. Cuando se sobrepasa este valor, el desencadenante de espacio crea nuevos volúmenes. El hecho de haberse excedido el umbral podría no generar la creación de nuevos volúmenes hasta que se realice la siguiente petición de espacio.


Puede determinar la utilización de la agrupación de almacenamiento ejecutando el mandato QUERY STGPOOL con FORMAT=DETAILED. El porcentaje de utilización de la agrupación de almacenamiento se visualiza en el campo "Util. desencadenante espacio". El cálculo de este porcentaje no incluye volúmenes reutilizables potenciales. El cálculo de la utilización del porcentaje que se utiliza para la migración y la reclamación, no obstante, sí incluye los volúmenes reutilizables potenciales.

SPACEexpansion

Para las agrupaciones de almacenamiento de tipo FILE de acceso secuencial, este parámetro se utiliza para determinar el número de volúmenes adicionales que se crean en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es 20. Los volúmenes se crean utilizando el valor MAXCAPACITY de la clase de dispositivo de la agrupación de almacenamiento. Para las agrupaciones de almacenamiento DISK de acceso aleatorio, el desencadenante de espacio crea un único volumen utilizando EXPANSIONPREFIX.


EXPansionprefix

Para las agrupaciones de almacenamiento DISK de acceso aleatorio, este parámetro especifica el prefijo que el servidor utiliza para crear nuevos archivos de agrupación de almacenamiento. Este parámetro es opcional y sólo se aplica a la clase de dispositivo DISK de acceso aleatorio. El prefijo predeterminado es la ruta de instalación del servidor.



El prefijo puede incluir uno o varios caracteres de separación de directorios; por ejemplo:  Sistemas operativos AIX


 Sistemas operativos Linux

```
/opt/tivoli/tsm/server/bin/
```

 Sistemas operativos Windows

```
c:\Archivos de programa\tivoli\tsm\
```

 Sistemas operativos AIX  Sistemas operativos Linux Puede especificar hasta 250 caracteres. Si especifica un prefijo erróneo, es posible que la ampliación automática no se ejecute.

 Sistemas operativos Windows Puede especificar hasta 200 caracteres. Si especifica un prefijo erróneo, es posible que la ampliación automática no se ejecute. Si el servidor se ejecuta como servicio de Windows, el prefijo predeterminado es el directorio c:\wnnt\system32.

Este parámetro no es válido para desencadenantes de espacio de agrupaciones de almacenamiento de acceso secuencial FILE. Los prefijos se obtienen de los directorios que se han especificado con la clase de dispositivo asociada.

STGPOOL

Especifica la agrupación de almacenamiento que está asociada con este desencadenante de espacio. Este parámetro es opcional para los desencadenantes de espacio de agrupación de almacenamiento. Si especifica el parámetro STG pero no se especifica el parámetro STGPOOL, se crea un desencadenante de espacio que se aplica a todas las agrupaciones de almacenamiento DISK (de acceso aleatorio) y FILE (de acceso secuencial) que no tienen un desencadenante de espacio específico.

Este parámetro no se aplica a agrupaciones de almacenamiento con el parámetro RECLAMATIONTYPE=SNAPLOCK.

Ejemplo: definir un desencadenante de espacio que incremente el espacio de la agrupación de almacenamiento un 25 por ciento

Establecer un desencadenante de espacio de agrupación de almacenamiento para que la cantidad de espacio de una agrupación de almacenamiento se incremente un 25 por ciento cuando se alcance un porcentaje de utilización de los volúmenes existentes equivalente al 80 por ciento. El espacio se crea en los directorios asociados con la clase de dispositivo.

```
define spacetrigger stg spaceexpansion=25 stgpool=file
```

Ejemplo: definir un desencadenante de espacio que incremente el espacio de la agrupación de almacenamiento un 40 por ciento

Establecer un desencadenante de espacio para la agrupación de almacenamiento WINPOOL1 para que la cantidad de espacio de la agrupación de almacenamiento se incremente un 40 por ciento cuando se alcance un porcentaje de utilización de los volúmenes existentes equivalente al 80 por ciento.

```
define spacetrigger stg spaceexpansion=40 stgpool=winpool1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SPACETRIGGER

Mandato	Descripción
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)

Utilice este mandato para definir un nuevo umbral de supervisión de estado.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STATusthreshold--nombre_umbral--actividad----->
. -Condition----EXists-----
>+-----+-----+-----+-----+-----+----->
' -Condition----+EXists--+' '-Value----valor-'
      +-GT-----+
      +-GE-----+
      +-LT-----+
      +-LE-----+
      '-Equal--'

. -Status----Normal-----
>+-----+-----+-----+-----+-----+-----<<
' -Status----+Normal--+'
      +-Warning-+
      '-Error--'
```

Parámetros

nombre_umbral (Necesario)

Especifica el nombre de umbral. El nombre de no puede tener más 48 caracteres de longitud.

actividad (Necesario)

Especifica la actividad para la que desea crear indicadores de estado. Especifique uno de los siguientes valores:

PROCESSSUMMARY

Especifica el número de procesos que están activos actualmente.

SESSIONSUMMARY

Especifica el número de sesiones que están activas actualmente.

CLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente que están activas actualmente.

SCHEDCLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente planificadas.

DBUTIL

Especifica el porcentaje de utilización de base de datos. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DBFREESPACE

Especifica el espacio libre disponible en la base de datos en gigabytes.

DBUSEDSPACE

Especifica la cantidad de espacio de base de datos que se utiliza, en gigabytes.

ARCHIVELOGFREESPACE

Especifica el espacio libre que está disponible en el registro de archivo, en gigabytes.

STGPOOLUTIL

Especifica el porcentaje de utilización de agrupación de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

STGPOOLCAPACITY

Especifica la capacidad de agrupación de almacenamiento en gigabytes.

AVGSTGPOOLUTIL

Especifica el porcentaje medio de utilización de agrupación de almacenamiento en todas las agrupaciones de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

TOTSTGPOOLCAPACITY

Especifica la capacidad total de agrupación de almacenamiento en gigabytes para todas las agrupaciones de almacenamiento disponibles.

TOTSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas.

TOTRWSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas que se puede leer o en las que se puede escribir.

TOTNOTRWSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas que no se pueden leer o en las que no se puede escribir.

STGPOOLINUSEANDDEFINED

Especifica el número total de volúmenes definidos que se están utilizando.

ACTIVELOGUTIL

Especifica el porcentaje de utilización actual del registro activo. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

ARCHLOGUTIL

Especifica la utilización actual del registro de archivado. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

CPYSTGPOOLUTIL

Especifica el porcentaje de utilización para una agrupación de almacenamiento de copia. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

PMRYSTGPOOLUTIL

Especifica el porcentaje de utilización para una agrupación de almacenamiento primario. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DEVCLASSPCTDRVOFFLINE

Especifica el porcentaje de utilización de las unidades que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDRVPOLLING

Especifica el sondeo de unidades, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTLIBPATHSOFFLINE

Especifica las rutas de biblioteca que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTPATHSOFFLINE

Especifica el porcentaje de rutas de clase de dispositivo que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDISKSNOTRW

Especifica el porcentaje de discos que no se pueden grabar para la clase de dispositivo de disco. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDISKSUNAVAILABLE

Especifica el porcentaje de volúmenes de disco que no están disponibles, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

FILEDEVCLASSPCTSCRUNALLOCATABLE

Especifica el porcentaje de volúmenes reutilizables que el servidor no puede asignar para una determinada clase de dispositivo de archivo no compartido. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

Condition

Especifica la condición que se utiliza para comparar la salida de actividad con el valor especificado. El valor predeterminado es EXISTS. Especifique uno de los siguientes valores:

EXists

Crea un indicador de supervisión de estado si existe la actividad.

GT

Crea un indicador de supervisión de estado si la salida de actividad es mayor que el valor especificado.

GE

Crea un indicador de supervisión de estado si la salida de actividad es mayor que o igual al valor especificado.

LT

Crea un indicador de supervisión de estado si la salida de actividad es menor que el valor especificado.

LE

Crea un indicador de supervisión de estado si la salida de actividad es menor que o igual al valor especificado.

EQual

Crea un indicador de supervisión de estado si la salida de actividad es igual al valor especificado.

Value (necesario)

Especifica el valor que se compara con la salida de actividad para la condición especificada. Debe especificar este parámetro, a menos que CONDITION esté establecido en EXISTS. Puede especificar un entero en el rango 0 – 9999999999999999.

Status

Especifica que se cree el indicador de estado en la supervisión de estado si pasa la condición que se está evaluando. Este parámetro opcional tiene un valor predeterminado de NORMAL. Especifique uno de los siguientes valores:

Normal

Especifica que el indicador de estado tiene un valor de estado normal.

Aviso

Especifica que el indicador de estado tiene un valor de estado de aviso.

Error

Especifica que el indicador de estado tiene un valor de estado de error.

Definir umbral de estado

Defina un umbral de estado para el porcentaje medio de utilización de agrupación de almacenamiento emitiendo el mandato siguiente:

```
define statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=85 condition=gt status=warning
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE STATUSTHRESHOLD

Mandato	Descripción
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

DEFINE STGPOOL (Definir una agrupación de almacenamiento)

Utilice este mandato para definir una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia, una agrupación de datos activos, una agrupación de almacenamiento de contenedor de directorio, una agrupación de almacenamiento de copia de contenedor, o una agrupación de almacenamiento de contenedor en un entorno de nube.

Una agrupación de almacenamiento primaria proporciona un destino para copias de seguridad de los archivos, copias archivadas o archivos que se han migrado desde los nodos de cliente. Una agrupación de almacenamiento de copia proporciona un destino para copias de los archivos que se encuentran en agrupaciones de almacenamiento primarias. Una agrupación de datos activos proporciona un destino para las versiones activas de datos de copia de seguridad que se encuentran en las agrupaciones de almacenamiento primarias. Una agrupación de almacenamiento de contenedor proporciona un destino para los archivos con duplicados eliminados. Una agrupación de almacenamiento en la nube proporciona el almacenamiento en un entorno de nube. Una agrupación de almacenamiento de copia de contenedor proporciona una copia en cinta de una agrupación de almacenamiento de contenedor de directorio. El número máximo de agrupaciones de almacenamiento que puede definir para un servidor es 999.

Todos los volúmenes de una agrupación de almacenamiento pertenecen a la misma clase de dispositivo. Las agrupaciones de almacenamiento de acceso aleatorio utilizan el tipo de dispositivo DISK. Después de definir una agrupación de almacenamiento de acceso aleatorio, debe definir los volúmenes de la agrupación para crear el espacio de almacenamiento.

Las agrupaciones de almacenamiento de acceso secuencial utilizan las clases de dispositivo definidas para dispositivos de cinta, archivos en disco (tipo de dispositivo FILE) y el almacenamiento en otro servidor (tipo de dispositivo SERVER). Para crear espacio de almacenamiento en una agrupación de almacenamiento de acceso secuencial debe permitir los volúmenes reutilizables para la agrupación al definirla o actualizarla, o bien definir volúmenes para la agrupación después de definirla. También puede hacer ambas cosas.

Restricción: Si un cliente utiliza la función de escritura simultánea y la deduplicación de datos, la función de deduplicación de datos se desactiva durante el proceso de copia de seguridad en una agrupación de almacenamiento.

El mandato DEFINE STGPOOL tiene seis formatos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con DEFINE STGPOOL

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
MOVE MEDIA	Mueve los volúmenes de agrupaciones de almacenamiento gestionados por una biblioteca automatizada.

Mandato	Descripción
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RENAME STGPOOL	Redenomina una agrupación de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de contenedores en la nube)
Utilice este mandato para definir una agrupación de almacenamiento de contenedor en un entorno de nube. Este tipo de agrupación de almacenamiento se utiliza para la eliminación de duplicados de datos. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de contenedores de directorio)
Utilice este mandato para definir una agrupación de almacenamiento de contenedores de directorio que se utilice para la deduplicación de datos.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de copia de contenedor)
Utilice este mandato para definir una agrupación de almacenamiento de copia de contenedor para que contenga una copia de datos de una agrupación de almacenamiento de contenedor de directorios.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio)
Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial)
Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial)
Utilice este mandato para definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial.
- **DEFINE STGPOOL** (Definir una agrupación de datos activos asignada a dispositivos de acceso secuencial)
Utilice este mandato para definir una agrupación de almacenamiento de datos asignada a dispositivos de acceso secuencial.

DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores en la nube)

Utilice este mandato para definir una agrupación de almacenamiento de contenedor en un entorno de nube. Este tipo de agrupación de almacenamiento se utiliza para la eliminación de duplicados de datos. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.

Consejo: Para optimizar el rendimiento de archivado y copia de seguridad, configure uno o varios directorios de almacenamiento local para contener temporalmente los datos que IBM Spectrum Protect está transfiriendo a la nube. Después de utilizar un mandato **DEFINE STGPOOL** para definir una agrupación de almacenamiento de contenedores en la nube, utilice el mandato **DEFINE STGPOOLDIRECTORY** para asignar directorios de almacenamiento local a la agrupación de almacenamiento de contenedores en la nube. Para obtener más información, consulte el apartado Optimización del rendimiento para el almacenamiento de objetos en la nube.

Consejo: Para optimizar el rendimiento, configure un directorio de almacenamiento local para contener temporalmente los datos que se muevan a la nube. Después de definir una agrupación de almacenamiento de contenedor en la nube, utilice el mandato DEFINE STGPOOLDIRECTORY para asignar directorios locales a la agrupación de almacenamiento de contenedor en la nube.

POoltype=Primary

Especifica que desea definir una agrupación de almacenamiento primaria. Este parámetro es opcional.

DESCription

Especifica una descripción de la agrupación de almacenamiento en la nube. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

CLOUDType

Especifica el tipo de entorno de nube donde está configurando la agrupación de almacenamiento.

Puede especificar uno de los siguientes valores:

AZure

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing Microsoft Azure.

S3

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing con el protocolo de servicio de almacenamiento simple (S3), como IBM® Cloud Object Storage o Amazon Web Services (AWS) S3. Si define una agrupación de almacenamiento como que utiliza S3 con este parámetro, no puede cambiar más adelante el tipo de agrupación de almacenamiento utilizando el mandato UPDATE STGPOOL.

SOftlayer

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing IBM SoftLayer (IBM Bluemix) con un sistema cloud computing OpenStack Swift.

SWift

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 2 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

V1Swift

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

Este parámetro es opcional. Si no especifica el parámetro, se utiliza el valor predeterminado SWIFT.

CLOUDUrl

Especifica el URL del entorno de nube donde está configurando la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un punto final de servicio blob, una URL de punto final de región, una dirección IP de accesor, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo `https://` o `http://`, al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL no se valida hasta que empieza la primera copia de seguridad.

Para obtener más información sobre cómo encontrar estos valores, seleccione su proveedor de servicios en la nube de la lista que aparece en la página Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos.

Consejo: Para utilizar más de un acceso de IBM Cloud Object Storage, liste las direcciones IP separadas por una barra vertical (|) sin espacios intercalados, como en el ejemplo siguiente:

```
CLOUDURL=<acceso_URL1>|<acceso_URL2>|<acceso_URL3>
```

Si va a utilizar el centro de operaciones, escriba una dirección IP de aplicación de acceso en el campo URL del asistente Añadir agrupación de almacenamiento y, a continuación, pulse Intro para añadir direcciones IP adicionales. Utilice varias aplicaciones de acceso para mejorar el rendimiento.

Este parámetro es necesario si especifica el parámetro CLOUDTYPE.

- AZure
- S3 (Simple Storage Service)
- SOftlayer
- SWift
- V1Swift

IDentity

Especifica el ID de usuario para la nube que se ha especificado en el parámetro STGTYPE=CLOUD. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si ha especificado CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

PAssword (Obligatorio)

Especifica la contraseña para la nube especificada en el parámetro STGTYPE=CLOUD. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar

para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres. Los parámetros IDENTITY y PASSWORD no se validan hasta que empieza la primera copia de seguridad.

CLOUDLocation

Especifica la ubicación física de la nube especificada en el parámetro CLOUD. Este parámetro es opcional. El valor predeterminado es OFFPREMISE. Puede especificar uno de los siguientes valores:

- OFFpremise
- ONpremise

BUCKETName

Especifica el nombre de un grupo de AWS S3 o una caja fuerte de IBM Cloud Object Storage que se van a utilizar con esta agrupación de almacenamiento, en lugar de utilizar el nombre de grupo o el nombre de caja fuerte predeterminados. Este parámetro es opcional y sólo es válido si especifica CLOUDTYPE=S3. Si no existe el nombre que especifica, el servidor crea un grupo o caja fuerte con el nombre especificado antes de utilizar el grupo o caja fuerte. Siga las restricciones de asignación de nombres de su proveedor de nube cuando especifique este parámetro. Revise los permisos del grupo o caja fuerte y asegúrese de que las credenciales de esta agrupación de almacenamiento tienen permiso de lectura, grabación, lista y supresión de objetos en este grupo o caja fuerte. Si no tiene la posibilidad de cambiar o ver los permisos, y todavía no ha grabado datos en esta agrupación de almacenamiento, utilice el mandato UPDATE STGPOOL con el parámetro BUCKETNAME para utilizar un grupo o caja fuerte diferente.

ACCess

Especifica cómo acceden los nodos cliente y los procesos de servidor a la agrupación de almacenamiento en la nube. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar uno de los siguientes valores:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en la agrupación de almacenamiento en la nube. Este es el valor predeterminado.

READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en la agrupación de almacenamiento en la nube.

UNAVailable

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento en la nube.

MAXWriters

Especifica el número máximo de sesiones de grabación que se pueden ejecutar simultáneamente en la agrupación de almacenamiento en la nube. Especifique un número máximo de sesiones de grabación para controlar que el rendimiento de la agrupación de almacenamiento en la nube no afecte negativamente a otros recursos del sistema. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que no existe un límite de tamaño máximo para el número de grabadores que puede utilizar. Este es el valor predeterminado.

máximo_grabadores

Limita el número máximo de grabadores que puede utilizar. Especifique un número entero del 1 al 99999.

REUsedelay

Especifica el número de días que deben transcurrir después de que se hayan eliminado todas las extensiones deduplicadas de una agrupación de almacenamiento en la nube. Este parámetro controla la duración con que las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento en la nube. Cuando caduca el valor especificado para este parámetro las extensiones deduplicadas se suprimen de la agrupación de almacenamiento en la nube. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento en la nube pasado un día. Este es el valor predeterminado.

días

Puede especificar un entero en el rango 0 – 9999.

Consejo: Defina este parámetro en un valor que sea mayor que el número especificado para el mandato SET DRMDBBACKUPEXPIREDAYS. Si establece este parámetro en un valor superior, puede garantizar que restaura la base de datos a un nivel anterior, las referencias a los archivos en la agrupación de almacenamiento en la nube siguen siendo válidas.

ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.
No

Especifica que el servidor no cifra los datos de cliente.

Este parámetro es opcional. El valor predeterminado depende de la ubicación física de la nube, que se especifica mediante el parámetro CLOUDLOCATION. Si la nube está fuera de las instalaciones, el servidor cifra los datos de forma predeterminada. Si la nube está en las instalaciones, el servidor no cifra los datos de forma predeterminada.

COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

Ejemplo 1: Definir una agrupación de almacenamiento de contenedores en la nube OpenStack Swift

Definir una agrupación de almacenamiento OpenStack Swift en la nube denominada STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password description="OpenStack Swift cloud"
```

Ejemplo 2: Definir una agrupación de almacenamiento primaria en un contenedor en la nube

Defina un contenedor de la agrupación de almacenamiento primaria que se denomina STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 pooltype=primary
```

Ejemplo 3: definir una agrupación de almacenamiento de contenedor en la nube con acceso de sólo lectura

Definir una agrupación de almacenamiento de contenedor en la nube denominada STGPOOL1 con acceso sólo lectura.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 access=readonly
```

Ejemplo 4: definir una agrupación de almacenamiento de contenedor en la nube con 99 sesiones de escritura

Defina una agrupación de almacenamiento de contenedor en la nube denominada STGPOOL1 con 99 sesiones de escritura.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 maxwr=99
```

Ejemplo 5: definir una agrupación de almacenamiento de contenedor en la nube en la que las extensiones con duplicados eliminados se supriman después de dos días

Definir una agrupación de almacenamiento de contenedor en la nube denominada STGPOOL1 en la que las extensiones con duplicados eliminados se supriman después de dos días.




```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 reusedelay=2
```

Tareas relacionadas:

Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos

Información relacionada:

Optimización del rendimiento para el almacenamiento de objetos en la nube

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio)

Utilice este mandato para definir una agrupación de almacenamiento de contenedores de directorio que se utilice para la deduplicación de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--STGType-----DIrectory----->
. -Pooltype-----Primary-.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -Pooltype-----Primary-' ' -DESCRiption-----descripción-'
. -ACCess-----READWrite------.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -ACCess-----+READWrite-----+
      +-READOnly-----+
      ' -UNAVailable-'
. -MAXSIze-----NOLimit------.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -MAXSIze-----+NOLimit-----+-----+
      ' -tamaño_máximo_archivo-'
. -MAXWriters-----NOLimit------.
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -MAXWriters-----+NOLimit-----+-----+
      ' -máximo_grabadores-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -NEXTstgpool-----nombre_agrupación-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -PROTECTstgpool-----agrup_almac_destino-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
|                                     .-./-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
|                                     v                                     | |
' -PROTECTLOCALstgpool-----agrupación_almacenamiento_destino_local+-----'
. -REUsedelay-----1----- . -ENCRypt-----No----- .
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -REUsedelay-----días-' ' -ENCRypt-----+Yes+-----
                                     ' -No--'
. -COMPReSSion-----Yes----- .
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -COMPReSSion-----+Yes+-----
                                     ' -No--'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento a definir. Este parámetro es necesario. La longitud máxima del nombre es de 30 caracteres.

STGType=DIrectory (Obligatorio)

Especifica el tipo de almacenamiento que desea definir para una agrupación de almacenamiento. Este parámetro especifica que a la agrupación de almacenamiento se le asigna un tipo de agrupación de almacenamiento de contenedor de directorio. Debe definir un directorio de agrupaciones de almacenamiento para este tipo de agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.

Requisitos:

- Asegúrese de que hay disponible espacio suficiente en el sistema de archivos para la agrupación de almacenamiento del contenedor de directorios.
- Debe almacenar la agrupación de almacenamiento de contenedores de directorio y la base de datos DB2 en puntos de montaje distintos en el sistema de archivos. La agrupación de almacenamiento de contenedores de directorio podría crecer hasta ocupar todo el espacio del directorio en el que está almacenada.
- Debe utilizar un sistema de archivos distinto al sistema de archivos donde se encuentra el servidor IBM Spectrum Protect.

POoltype=Primary

Especifica que desea que la agrupación de almacenamiento se utilice como una agrupación de almacenamiento primaria. Este parámetro es opcional.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo pueden los nodos de cliente y los procesos de servidor acceder a la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

READWrite

Especifica que los nodos de cliente y los procesos de servidor pueden realizar operaciones de lectura y grabación en la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en la agrupación de almacenamiento.

UNAVailable

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento.

MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

tamaño_máximo_archivo

Limita el tamaño máximo de archivo físico. Puede especificar un entero del 1 al 999999, seguido de un factor de ajuste proporcional. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo para esta agrupación de almacenamiento son 5 GB. Puede utilizar una de las siguientes unidades de medida:

Tabla 1. Factor de escala para el tamaño de archivo máximo

Factor de escala	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

Consejo: Si no especifica una unidad de medida para el tamaño máximo de archivo, el valor se especifica en bytes.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 2. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

Agrupación especificada	Resultado
No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor no almacena el archivo.
Se ha especificado una agrupación como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor almacena el archivo en la agrupación de almacenamiento que ha especificado.

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos durante el proceso de deduplicación de datos, el servidor considera que el tamaño del proceso de deduplicación de datos es el tamaño de archivo. Si el tamaño total de todos los archivos del proceso es mayor que el límite de

tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

MAXWriters

Especifica el número máximo de hebras de E/S para los siguientes procesos:

- El número de hebras de E/S que se pueden ejecutar simultáneamente en la agrupación de almacenamiento de contenedores de directorio.
- El número de hebras de E/S que se graban simultáneamente en la agrupación de almacenamiento de contenedores de directorio.

Este parámetro es opcional. Como práctica recomendada, utilice el valor predeterminado NOLIMIT. Puede especificar los valores siguientes:

NOLimit

Especifica que no se graba ningún número máximo de hebras de E/S en la agrupación de almacenamiento.

máximo_grabadores

Limita el número máximo de hebras de E/S que puede utilizar. Especifique un número entero del 1 al 99999.

Consejo: El servidor de IBM Spectrum Protect gestiona el número de hebras de E/S de forma automática en función de los recursos que hay disponibles y la carga del servidor.

NEXTstgpool

Especifica el nombre de una agrupación de almacenamiento secuencial primaria o de acceso aleatorio en la que se almacenan los archivos cuando la agrupación de almacenamiento de contenedores de directorio está llena. Este parámetro es opcional.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

PROTECTstgpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino donde se realiza la copia de seguridad de los datos cuando utiliza el mandato PROTECT STGPOOL para esta agrupación de almacenamiento. Este parámetro es opcional.

PROTECTLOCALstgpools

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor en un dispositivo local en el que se realiza la copia de seguridad de los datos. Esta agrupación de almacenamiento de copia de contenedor será una agrupación de almacenamiento de destino local cuando utilice el mandato PROTECT STGPOOL. Puede especificar un máximo de dos nombres de agrupación de almacenamiento de copia de contenedor. Puede separar varios nombres con comas y sin espacios intercalados. La longitud máxima de cada nombre es de 30 caracteres. Este parámetro es opcional.

REUsedelay

Especifica el número de días que deben transcurrir antes de que se eliminen todas las extensiones con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio. Este parámetro controla el tiempo durante el cual las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento de contenedores de directorio después de que ya no se haga referencia a ellas. Cuando expira el período de tiempo especificado para el parámetro, las extensiones con duplicados eliminados se suprimen de la agrupación de almacenamiento de contenedores de directorio. Especifique un número entero del 0 al 9999. El valor predeterminado para las agrupaciones de almacenamiento de contenedores de directorio es 1, lo que significa que las extensiones con duplicados eliminados a las que ya no se hace referencia se suprimen de una agrupación de almacenamiento de contenedores de directorio al cabo de 1 día.

Establezca este parámetro en un valor mayor que el número especificado como periodo de copia de seguridad de base de datos, para asegurarse de que las extensiones de datos continúan siendo válidas cuando restaura la base de datos a otro nivel.

ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente. Este es el valor predeterminado.

COMPReSSion

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio configurada para almacenamiento de desbordamiento para cuando la agrupación de almacenamiento está llena

Definir una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL1. La agrupación de almacenamiento está configurada para que el almacenamiento se desborde en una agrupación de almacenamiento de cinta cuando la agrupación de almacenamiento este llena.

```
define stgpool stgpool1 stgtype=directory nextstgpool=overflow_tape_pool
```

Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio que especifique el tamaño máximo de archivo

Defina una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL2. La agrupación de almacenamiento especifica el tamaño máximo de archivo que el servidor puede almacenar en la agrupación de almacenamiento en 100 megabytes.

```
define stgpool stgpool2 stgtype=directory maxsize=100M
```

Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen con una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino para hacer copia de seguridad de los datos

Defina una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL3. Se hace una copia de seguridad de los datos de la agrupación de almacenamiento STGPOOL3 en una agrupación de almacenamiento de contenedores de directorio, TARGET_STGPOOL3, en el servidor de réplica de destino.

```
define stgpool stgpool3 stgtype=directory protectstgpool=target_stgpool3
```

Ejemplo: defina una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen con una agrupación de almacenamiento de copia de directorios para hacer una copia de seguridad local de los datos

Defina una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL3. Se hace una copia de seguridad de los datos de la agrupación de almacenamiento STGPOOL3 en una agrupación de almacenamiento de copia de contenedor local, TARGET_LOCALSTGPOOL.

```
define stgpool stgpool3 stgtype=directory protectlocalstgpools=target_localstgpool
```

Ejemplo: Definir una agrupación de almacenamiento de contenedor de directorio e inhabilitar la compresión

Defina una agrupación de almacenamiento de contenedor de directorio denominada STGPOOL1 e inhabilite la compresión.

```
define stgpool stgpool1 stgtype=directory compression=no
```

Tabla 3. Mandatos relacionados con DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio)

Mandato	Descripción
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY CONTAINER	Visualiza información sobre un contenedor.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.

Mandato	Descripción
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (contenedor de directorios)	Actualizar una agrupación de almacenamiento de contenedores de directorios.

DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia de contenedor)

Utilice este mandato para definir una agrupación de almacenamiento de copia de contenedor para que contenga una copia de datos de una agrupación de almacenamiento de contenedor de directorios.

Clase de privilegio

Para emitir este mandato, debe tener privilegios de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
>--POoltype-----COPYCONtainer--MAXSCRatch-----número----->
>+-----+-----+----->
  '-DESCRiption-----descripción-'
  .-ACCess-----READWrite-----
>+-----+-----+----->
  '-ACCess-----+READWrite---+'
                    +-READOnly-----+
                    '-UNAVailable-'

  .-PROTECTProcess-----2----- .-REClaim-----100-----
>+-----+-----+----->
  '-PROTECTProcess-----número-' '-REClaim-----porcentaje-'

  .-RECLAIMLIMit-----NOLimit-----
>+-----+-----+----->
  '-RECLAIMLIMit-----+NOLimit---+'
                    '-límite_vol-'

  .-REUsedelay-----0-----
>+-----+-----+-----><
  '-REUsedelay-----días-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial a la que se asigna esta agrupación de almacenamiento.

Restricción: No puede especificar los tipos de clase de dispositivo siguientes:

- DISK
- FILE
- CENTERA
- NAS
- REMOVABLEFILE
- SERVER

Restricción: Las bibliotecas de cintas virtuales no están soportadas, independientemente del tipo de biblioteca que se defina.

Solo recibe soporte la cinta física.

POoltype=COPYCONtainer (Obligatorio)

Especifica que desea definir una agrupación de almacenamiento de copia de contenedor. Una agrupación de almacenamiento de copia de contenedor se utiliza sólo para almacenar una copia de datos de una agrupación de almacenamiento de contenedor de directorios.

MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero en el rango 0 - 100000000. Si el servidor puede solicitar volúmenes reutilizables según sean necesarios, no tiene que definir cada volumen que se va a utilizar.

El valor de este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprime de la agrupación de almacenamiento mientras no se cambie la modalidad de acceso. A continuación, un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo pueden acceder a los datos de la agrupación de almacenamiento los procesos como por ejemplo la protección y la reparación de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar uno de los siguientes valores:

READWrite

Especifica que el servidor puede leer y grabar en volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que el servidor sólo puede leer volúmenes de la agrupación de almacenamiento. El servidor puede utilizar datos de la agrupación de almacenamiento para restaurar extensiones en agrupaciones de almacenamiento de contenedor de directorios. No se permiten operaciones que graban en la agrupación de almacenamiento de contenedor de directorios.

UNAVailable

Especifica que el servidor no puede acceder a los datos almacenados en volúmenes de la agrupación de almacenamiento.

PROTECTProcess

Especifica el número máximo de procesos paralelos que se utilizan cuando se emite el mandato PROTECT STGPOOL para copiar datos en esta agrupación desde una agrupación de almacenamiento de contenedor de directorios. Este parámetro es opcional. Especifique un valor del 1 al 20. El valor predeterminado es 2.

El tiempo que es necesario para realizar la operación de copia se puede reducir utilizando varios procesos paralelos. Sin embargo, en algunos casos, cuando se ejecutan varios procesos, uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso distinto.

Cuando especifique este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a la operación de copia. Para acceder a un volumen de cinta, el servidor utiliza un punto de montaje y una unidad. El número de puntos de montaje y unidades disponibles depende del límite de montaje de la clase de dispositivo de la agrupación de almacenamiento y de otra actividad del servidor y del sistema.

Este parámetro se ignora si utiliza la opción PREVIEW=YES en el mandato PROTECT STGPOOL. En ese caso, sólo se utiliza un proceso y no se necesitan puntos de montaje ni unidades.

REClaim

Especifica cuando un volumen pasa a ser seleccionable para la reclamación y la reutilización. Especifica la elegibilidad como el porcentaje de espacio de un volumen que está ocupado por las extensiones que ya no se almacenan en la agrupación de almacenamiento de contenedor de directorios. La reclamación mueve cualesquiera extensiones que sigan almacenadas en la agrupación de almacenamiento de contenedor de directorios de volúmenes elegibles a otros volúmenes. La reclamación se produce sólo cuando un mandato PROTECT STGPOOL almacena datos en esta agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero en el rango 1 - 100. El valor predeterminado es 100, lo que significa que los volúmenes de esta agrupación de almacenamiento no se reclaman.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Al establecer un valor de reclamación de 50 o superior, los datos que se mueven de dos volúmenes reclamados no utilizan más del equivalente de un nuevo volumen.

Tenga cuidado al utilizar la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Por lo tanto, para fines de recuperación ante siniestro, asegúrese de que planifica las copias de seguridad de bases de datos para que se ejecuten después de que se hayan ejecutado las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM, y asegúrese de que todos los volúmenes de copia de seguridad de bases de datos se trasladen fuera del local junto con los volúmenes de DRM.

Consejo: Establezca diferentes valores de reclamación para las agrupaciones de almacenamiento de copia de contenedor fuera del local y dentro del local. Debido a que las agrupaciones de almacenamiento de copia de contenedor almacenan datos de eliminación de duplicados, las extensiones de datos abarcan varios volúmenes de cinta. Cuando seleccione un umbral de reclamación para una copia fuera del local, tenga en cuenta el número de puntos de montaje disponibles y el número de volúmenes de cinta que debe recuperar en caso de siniestro. Establecer un umbral más alto, significa que se deberán recuperar más volúmenes que si se establece la reclamación en un valor inferior. Si se utiliza un umbral más bajo se reduce el número de puntos de montaje necesarios en caso de siniestro. El método preferido consiste en definir el valor de reclamación para copias externas en 60 y, para copias internas, en el intervalo 90 - 100.

RECLAIMLimit

Especifica el número máximo de volúmenes que reclama el servidor cuando se emite el mandato PROTECT STGPOOL y se especifican las opciones RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED. Este parámetro solo es válido para las agrupaciones de almacenamiento de copia de contenedor. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que todos los volúmenes de la agrupación de almacenamiento de copia de contenedor se procesen para la reclamación.

límite_vol

Especifica el número máximo de volúmenes de la agrupación de almacenamiento de copia de contenedor que se reclaman. El valor que se especifique determinará cuántas nuevas cintas reutilizables están disponibles una vez completado el proceso de reclamación. Puede especificar un número comprendido entre 1 y 100000.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todas las extensiones de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva al estado reutilizable. Este parámetro es opcional. Puede especificar un entero en el rango 0 – 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo al estado reutilizable, tan pronto como se han suprimido todas las extensiones del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a extensiones de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. Si utiliza gestor recuperación ante siniestro, el número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDAYS.

Ejemplo: Definir una agrupación de almacenamiento de copia de contenedor con una clase de dispositivo LTO7A

Definir una agrupación de almacenamiento de copia de contenedor, CONTAINER1_COPY2, en la clase de dispositivo LTO7A. Se permitirán hasta 50 volúmenes reutilizables en esta agrupación. La reutilización de volúmenes se retardará 45 días.

```
define stgpool container1_copy2 lto7a pooltype=copycontainer
maxscratch=50 reusedelay=45
```

Tabla 1. Mandatos relacionados con DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia de contenedor)

Mandato	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.

Mandato	Descripción
UPDATE STGPOOL (copia de contenedor)	Actualizar una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (contenedor de directorios)	Actualizar una agrupación de almacenamiento de contenedores de directorios.

DEFINE STGPOOL (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio)

Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--DISK----->
. .-Pooltype----Primary-. .-STGType----Devclass-.
>--+-----+-----+-----+-----+----->
'-Pooltype----Primary-' '-STGType----Devclass-'

>--+-----+-----+-----+-----+----->
'-DESCription----descripción-'

. .-ACcEss----READWrite-----
>--+-----+-----+-----+-----+----->
'-ACcEss----+READWrite---+'
+READOnly----+
'-UNAVailable-'

. .-MAXSIze----NOLimit-----
>--+-----+-----+-----+-----+----->
'-MAXSIze----tamaño_máximo_archivo-'

. .-CRCDaTA----No-----
>--+-----+-----+-----+-----+----->
'-CRCDaTA----+Yes+-'
'-No--'

>--+-----+-----+-----+-----+----->
'-NEXTstgpool----nombre_agrupación-'

. .-HIghmig----90----- . .-LOwmig----70-----
>--+-----+-----+-----+-----+----->
'-HIghmig----percent-' '-LOwmig----percent-'

. .-CACHe----No----- . .-MIGPRocess----1-----
>--+-----+-----+-----+-----+----->
'-CACHe----+Yes+-' '-MIGPRocess----number-'
'-No--'

. .-MIGDelAy----0---- . .-MIGContInue----Yes-----
>--+-----+-----+-----+-----+----->
'-MIGDelAy----días-' '-MIGContInue----+Yes+-'
'-No--'

. .-AUTOCopy----ClIent-----
>--+-----+-----+-----+-----+----->
'-AUTOCopy----+None-----+'
+ClIent----+
+MIGRation+
'-All-----'

>--+-----+-----+-----+-----+----->
| .-,-----|
```

```


|           V           |   .-COPYContinue-----Yes-----.|
'-COPYSTGpools-----nombre_agrupación_copia+-----+-----+-'
                                     '-COPYContinue-----+Yes+-'
                                             '-No--'

>-----+----->
|           V           |   .-ACTIVEDATApools-----nombre_agrupación_datos_activos+---'
'-ACTIVEDATApools-----nombre_agrupación_datos_activos+---'

    .-SHRED-----0-----
>-----+-----<
|                                   (1) (2) |
'-SHRED-----recuento_sobregrabación-----'

```

Notas:

1. Este parámetro no está disponible en el caso de las agrupaciones de almacenamiento CENTERA o SnapLock.
2.  Sistemas operativos Linux Este parámetro no está disponible para las agrupaciones de almacenamiento SnapLock.

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de definir. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

DISK (Necesario)

Especifica que desea definir una agrupación de almacenamiento en la clase de dispositivo DISK (la clase de dispositivo se predefine durante la instalación).

POoltype=Primary

Especifica que desea definir una agrupación de almacenamiento primaria. Este parámetro es opcional. El valor predeterminado es PRIMARY.

STGType

Especifica el tipo de almacenamiento que desea definir para una agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es DEVCLASS.

Devclass

Especifica que se asigna un tipo de clase de dispositivo de agrupación de almacenamiento a la agrupación de almacenamiento.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin

embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

tamaño_máximo_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo para esta agrupación de almacenamiento son 5 GB. Puede utilizar una de las siguientes unidades de medida:

Factor de escala	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se produce una carga general adicional para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. Este parámetro es opcional. Si no especifica ninguna agrupación de almacenamiento siguiente, se producen las acciones siguientes:

- El servidor no puede migrar los archivos de esta agrupación de almacenamiento
- El servidor no puede almacenar archivos que superen el tamaño máximo de esta agrupación de almacenamiento en otra agrupación de almacenamiento

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

Highmig

Especifica que el servidor inicia la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 100. El valor predeterminado es 90.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por nodo a la siguiente agrupación de almacenamiento. El parámetro NEXTSTGPOOL define este valor. Puede especificar HIGHMIG=100 para impedir que se produzca la migración en esta agrupación de almacenamiento.

LOwmig

Especifica que el servidor detiene la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 99. El valor predeterminado es 70.

Cuando la migración se realiza por nodo o espacio de archivos, en función de la proximidad, el nivel de ocupación de la agrupación de almacenamiento puede caer por debajo del valor que ha especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0.

CAChe

Especifica si el proceso de migración deja una copia en caché de un archivo en esta agrupación de almacenamiento una vez migrado el archivo a la siguiente agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

Yes

Especifica que está activada la función de caché.

No

Especifica que está desactivada la función de caché.

Si se utiliza la función de caché se puede mejorar la posibilidad de recuperar archivos, pero puede afectar al rendimiento de otros procesos.

MIGProcess

Especifica el número de procesos que utiliza el servidor para migrar los archivos de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero del 1 al 999. El valor predeterminado es 1.

Durante la migración, estos procesos se ejecutan en paralelo para proporcionar el potencial de mejorar los índices de migración.

Consejos:

- El número de procesos de migración depende de los siguientes valores:
 - El parámetro MIGPROCESS
 - El valor de proximidad de la agrupación siguiente
 - El número de nodos o el número de grupos de proximidad con datos en la agrupación de almacenamiento que se está migrando

Por ejemplo, supongamos que tenemos MIGPROCESS =6, el parámetro COLLOCATE de la siguiente agrupación está establecido en NODE, pero solo hay dos nodos con datos en la agrupación de almacenamiento. El proceso de migración consta solo de dos procesos, no de seis. Si el parámetro COLLOCATE está establecido en GROUP y ambos nodos están en el mismo grupo, el proceso de migración consta solamente de un proceso. Si el parámetro COLLOCATE está establecido

en NO o FILESPACE, y cada nodo tiene dos espacios de archivos con datos de copia de seguridad, el proceso de migración consta de cuatro procesos.

- Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Para calcular un valor para comparar con el valor MIGDELAY especificado, el servidor cuenta los elementos siguientes:

- El número de días que el archivo ha estado en la agrupación de almacenamiento
- El número de días, si hay alguno, desde que un cliente recuperó el archivo

El menor de ambos valores se compara con el valor de MIGDELAY especificado. Por ejemplo, si se cumplen todas las condiciones siguientes, no se migrará un archivo:

- Un archivo ha permanecido en una agrupación de almacenamiento durante cinco días.
- Un cliente ha accedido al archivo en los tres últimos días.
- El valor especificado para el parámetro MIGDELAY es cuatro días.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración.

Si desea que el servidor cuente el número de días basándose tan solo en el momento en que se almacenó un archivo y no en el momento en el que se recuperó, utilice la opción del servidor NORETRIEVEDATE.

MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional. El valor predeterminado es YES.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. El valor predeterminado es CLIENT. Este parámetro es opcional y afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPOOLS. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPOLS.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea esta inhabilitada.

Client

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. El parámetro COPYSTGPOOLS es opcional. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Al especificar un valor para el parámetro COPYSTGPOOLS, también puede especificar un valor para el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricción: No se admite la función de grabación simultánea en las siguientes operaciones de almacenamiento:

- Cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
- Operaciones de copias de seguridad de NAS. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia:
 - Las agrupaciones de almacenamiento de copia se ignoran
 - Los datos solo se almacenan en la agrupación de almacenamiento primaria

Atención: La función que proporciona el parámetro COPYSTGPOOLS no tiene como finalidad sustituir el mandato BACKUP STGPOOL. Si utiliza el parámetro COPYSTGPOOLS, continúe utilizando el mandato BACKUP STGPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

COPYContinue

Especifica cómo reacciona normalmente el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOOLS. Este parámetro es opcional. El valor predeterminado es YES. Si especifica el parámetro COPYCONTINUE, también debe especificar el parámetro COPYSTGPOOLS.

Puede especificar los siguientes valores:

Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEDATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSGTPOOLS y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro solamente está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos "NATIVE" o "NONBLOCK". Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria especificada en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos:
 - Las agrupaciones de datos activos se ignoran
 - Los datos solo se almacenan en la agrupación de almacenamiento primaria
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el mandato COPY ACTIVEDATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVEDATAPOOLS no tiene como finalidad sustituir al mandato COPY ACTIVEDATA. Si utiliza el parámetro ACTIVEDATAPOOLS, utilice el mandato COPY ACTIVEDATA para garantizar que las

agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

SHRED

Especifica si los datos se van a sobregabar físicamente cuando se supriman. Este parámetro es opcional. Puede especificar un entero del 0 al 10. El valor predeterminado es 0.

Si especifica un valor de cero, el servidor suprime los datos de la base de datos. Sin embargo, el almacenamiento que se utiliza para contener los datos no se sobregaba, y los datos existirán en el almacenamiento hasta que se reutilice el almacenamiento para otros datos. Los datos se podrían descubrir y reconstruir tras haberlos suprimido.

Si especifica un valor mayor que cero, el servidor suprime los datos lógicamente y físicamente. El servidor sobregaba el almacenamiento utilizado para contener los datos el número especificado de veces. Esta sobregabación aumenta la dificultad de descubrir y reconstruir los datos tras su supresión.

Para asegurarse de que todas las copias de los datos se destruyen, especifique un valor SHRED superior a cero para la agrupación de almacenamiento especificada en el parámetro NEXTSTGPOOL. No especifique ni COPYSTGPOOLS ni ACTIVEDATAPOOLS. Normalmente la especificación de valores relativamente altos para el recuento de sobregabación mejora el nivel de seguridad, pero podría afectar negativamente al rendimiento.

La sobregabación de datos suprimidos se realiza de forma asíncrona tras completarse la operación de supresión. Por lo tanto, el espacio ocupado por los datos suprimidos permanecerá ocupado durante algún tiempo. El espacio no está disponible como espacio libre para nuevos datos.

No se puede utilizar un valor SHRED superior a cero si el valor del parámetro CACHE es YES.

Importante: Después de que haya finalizado una operación de exportación y se hayan identificado los archivos para la exportación, los cambios que se realicen en el valor SHRED se ignorarán. Una operación de exportación que se ha suspendido retiene el valor de SHRED original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor SHRED de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el mandato de exportación después de realizar la operación de limpieza necesaria.

Ejemplo: definir una agrupación de almacenamiento primaria para una clase de dispositivo DISK

Definir una agrupación de almacenamiento primaria, POOL1, que utilice la clase de dispositivo DISK, con la función de caché activada. Limitar el tamaño de archivo máximo a 5 MB. Almacenar los archivos de más de 5 MB en agrupaciones de almacenamiento subordinadas, que empiezan con la agrupación de almacenamiento PROG2. El umbral superior de migración se establecerá en el 70 % y el umbral inferior de migración en el 30 %.

```
define stgpool pool1 disk
description="main disk storage pool" maxsize=5m
highmig=70 lowmig=30 cache=yes
nextstgpool=prog2
```

DEFINE STGPOOL (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial)

Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
  .-POOLtype----PRimary-.  .-STGType----Devclass-.
>--+-----+-----+-----+-----+----->
  '-POOLtype----PRimary-'  '-STGType----Devclass-'

>--+-----+-----+-----+-----+----->
  '-DESCRiption----descripción-'

  .-ACCess----READWrite-----
>--+-----+-----+-----+-----+----->
  '-ACCess----+READWrite----+'
      +-READOnly----+
```


Especifica el tipo de almacenamiento que desea definir para una agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es DEVCLASS.

Devclass

Especifica que se asigna un tipo de clase de dispositivo de agrupación de almacenamiento a la agrupación de almacenamiento.

DEScRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

tamaño_máximo_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la

compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

Restricción:

Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. No puede migrar datos de una agrupación de almacenamiento de acceso secuencial a una agrupación de almacenamiento de acceso aleatorio. Este parámetro es opcional.

Si esta agrupación de almacenamiento no tiene una agrupación de almacenamiento que le siga, el servidor no puede migrar los archivos de esta agrupación de almacenamiento y no puede almacenar en otra agrupación de almacenamiento los archivos que sobrepasan el tamaño máximo de esta agrupación de almacenamiento.

Cuando no hay suficiente espacio disponible en la agrupación de almacenamiento actual, el parámetro NEXTSTGPOOL para las agrupaciones de almacenamiento de acceso secuencial no permite que los datos se almacenen en la agrupación siguiente. En este caso, el servidor emite un mensaje y la transacción no se efectúa correctamente.

Para las siguientes agrupaciones de almacenamiento con un tipo de dispositivo FILE, el servidor realiza una comprobación preliminar para determinar si hay disponible espacio suficiente. Si no hay espacio disponible, el servidor salta a la siguiente agrupación de almacenamiento de la jerarquía. Si hay espacio disponible, el servidor intenta almacenar datos en esa agrupación. No obstante, es posible que falle la operación de almacenamiento porque cuando se intenta realmente realizar la operación de almacenamiento el espacio ya no está disponible.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor de nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.
- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP

HIghmig

Especifica que el servidor inicia la migración cuando la utilización de la agrupación de almacenamiento alcanza este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 100. El valor predeterminado es 90.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por volumen, a la siguiente agrupación de almacenamiento definida para la agrupación. Puede establecer el umbral superior de migración en 100 para impedir la migración en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

LOwmig

Especifica que el servidor detiene la migración cuando la utilización de la agrupación de almacenamiento es igual o inferior a este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 99. El valor predeterminado es 70.

Cuando la agrupación de almacenamiento alcanza el umbral inferior de migración, el servidor no inicia la migración de los archivos de otro volumen. Puede establecer el umbral inferior de migración en 0 para permitir que la migración vacíe la agrupación de almacenamiento.



Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es 60, excepto para agrupaciones de almacenamiento que utilicen dispositivos WORM.

 Sistemas operativos AIX  Sistemas operativos Windows Para las agrupaciones de almacenamiento que utilizan dispositivos WORM, se puede bajar el valor predeterminado 100. Al bajar el valor, el servidor puede consolidar los datos en menos volúmenes cuando sea necesario. Los volúmenes que se vacían por la operación de reclamación se pueden dar de baja de la biblioteca, con lo que quedan ranuras libres para nuevos volúmenes. Los volúmenes no se pueden reutilizar porque son de una sola operación de grabación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMPRocess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1. Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento primaria de acceso secuencial.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que no se ha especificado el parámetro RECLAIMSTGPOOL o que la agrupación de almacenamiento de reclamación tiene la misma clase de dispositivo que la agrupación de almacenamiento que se reclama, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMSTGpool

Especifica otra agrupación de almacenamiento primaria como destino de los datos reclamados de esta agrupación de almacenamiento. Este parámetro es opcional. Cuando el servidor reclama volúmenes para la agrupación de almacenamiento, el servidor traspasa los datos sin caducar de los volúmenes que se están reclamando a la agrupación de almacenamiento indicada en este parámetro.

Una agrupación de almacenamiento de reclamación tiene la mayor utilidad para una agrupación de almacenamiento que sólo tenga una unidad en su biblioteca. Al especificar este parámetro, el servidor traspasa todos los datos de los volúmenes reclamados a la agrupación de almacenamiento de reclamación independientemente del número de unidades de la biblioteca.

Para volver a traspasar los datos de la agrupación de almacenamiento de reclamación a la agrupación de almacenamiento original, utilice la jerarquía de agrupaciones de almacenamiento. Especifique la agrupación de almacenamiento original como la siguiente agrupación de almacenamiento de la agrupación de almacenamiento de reclamación.

Restricción:

- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAMATIONType

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención por medio del software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido para agrupaciones de almacenamiento que están definidos en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El mandato DEFINE puede fallar si el parámetro RECLAMATIONTYPE especificado es distinto del que está definido para las agrupaciones de almacenamiento que ya están definidas en el nombre de clase de dispositivo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional. El valor predeterminado es GROUP.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario. La función de proximidad también pueden afectar al número de procesos de migración de discos a agrupación secuencial.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada. Durante la migración de disco, los procesos se crean a un nivel de espacio de archivos.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no añade nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para nodos agrupados, y en el nivel de nodo para nodos no agrupados.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos que se denominan A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para espacios de archivos agrupados.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Para COLLOCATE=NODE, el servidor crea procesos en el nivel de nodo cuando se migran datos del disco.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

Para COLLOCATE=FILESPACE, el servidor crea procesos en el nivel de espacio de archivos al migrar datos del disco.

MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables, se evita tener que definir cada volumen que se va a utilizar.

El valor especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Cuando se suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el mandato. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Todos los archivos de un volumen deben poder seleccionarse para una operación de migración antes de que el servidor seleccione el volumen para migración. Para calcular un valor para comparar con el valor MIGDELAY especificado, el servidor cuenta el número de días que el archivo ha permanecido en la agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración. Si desea que el servidor cuente el número de días sólo basándose en el momento en que se almacenó un archivo y no en el momento en que se recuperó, utilice la opción del servidor NORETRIEVEDATE.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional. El valor predeterminado es YES.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

MIGPRocess

Especifica el número de procesos paralelos que se utilizará para migrar los archivos de los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta el número de agrupaciones de almacenamiento secuenciales que participarán en la migración y el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la migración.

Por ejemplo, supongamos que desea migrar los volúmenes de dos agrupaciones de almacenamiento secuencial primarias simultáneamente y que desea especificar tres procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que la agrupación de almacenamiento a la que se están migrando los archivos tienen la misma clase de dispositivo que la agrupación de almacenamiento de la que se migran, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una unidad corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar simultáneamente seis procesos de migración, necesita como mínimo un total de 12 puntos de montaje y 12 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 12 como mínimo.

Si el número de procesos de migración especificados es mayor que el número de puntos de montaje o unidades disponibles, los procesos que no obtengan puntos de montaje o unidades esperarán a que haya puntos de montaje o unidades disponibles. Si las unidades o los puntos de montaje no pasan a estar disponibles dentro del tiempo MOUNTWAIT, los procesos de migración finalizarán. Para obtener información acerca de la especificación del tiempo MOUNTWAIT, consulte el apartado DEFINE DEVCLASS (Definir una clase de dispositivo).

El servidor de IBM Spectrum Protect iniciará el número especificado de procesos de migración independientemente del número de volúmenes elegibles para la migración. Por ejemplo, si especifica diez procesos de migración y sólo seis volúmenes son elegibles para migración, el servidor iniciará diez procesos y cuatro de ellos terminarán sin que se procesen volúmenes.

Consejo: Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

DATAFormat

Especifica el formato de datos que debe utilizarse para hacer copia de seguridad de archivos en esta agrupación de almacenamiento y restaurarlos de la misma. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

NATive

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

NETAPPDump

Especifica que los datos tienen un formato de vuelco NetApp. Este formato de datos se debe especificar para imágenes del sistema de archivos que están en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos NetApp o IBM System Storage N Series que utiliza NDMP. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NETAPPDUMP. Puede utilizar el mandato MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

CELERRADump

Especifica que los datos tienen un formato de vuelco EMC Celerra. Este formato de datos se debe especificar para las imágenes de sistema de archivos que tienen un formato de vuelco y de las que se realizó una copia de seguridad a partir de un servidor de archivos EMC Celerra que utiliza NDMP. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=CELERRADUMP. Puede utilizar el mandato MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

NDMPDump

Especifica que los datos tienen un formato de copia de seguridad específico del fabricante del NAS. Utilice este formato de datos para las imágenes de sistemas de archivos de las que se hizo una copia de seguridad desde un servidor de archivos NAS que no sea NetApp o EMC Celerra. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NDMPDUMP. Puede utilizar el mandato MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. El valor predeterminado es CLIENT. Este parámetro es opcional y afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si la opción AUTOCOPY se establece en ALL o CLIENT y existe como mínimo una agrupación de almacenamiento que aparece listada en las opciones COPYSTGPOOLS o ACTIVEDATAPOOLS, la eliminación de duplicados del lado del cliente está inhabilitada.

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPOOLS. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPOOLS.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea está inhabilitada.

Client

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los

procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. El parámetro COPYSTGPOOLS es opcional. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Al especificar un valor para el parámetro COPYSTGPOOLS, también puede especificar un valor para el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEPOOL no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento definida con una lista de agrupaciones de almacenamiento de copia.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
2. No se da soporte a la grabación simultánea en agrupaciones de almacenamiento de copia cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se da soporte a la grabación simultánea en las siguientes operaciones de almacenamiento. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia, éstas se pasarán por alto y los datos se almacenarán únicamente en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.

Atención: La función que proporciona el parámetro COPYSTGPOOLS no tiene como finalidad sustituir el mandato BACKUP STGPOOL. Si utiliza el parámetro COPYSTGPOOLS, continúe utilizando el mandato BACKUP STGPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOOLS. Este parámetro es opcional. El valor predeterminado es YES. Si especifica el parámetro COPYCONTINUE, también debe especificar el parámetro COPYSTGPOOLS.

El parámetro COPYCONTINUE no afecta a la función de grabación simultánea durante la migración.

Puede especificar los siguientes valores:

Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSGTPOOLS y ACTIVEATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento principal a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria que se ha especificado en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos, las agrupaciones de datos activos se pasarán por alto y los datos sólo se almacenarán en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el mandato COPY ACTIVEATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVEATAPOOLS no tiene como finalidad sustituir al mandato COPY ACTIVEATA. Si utiliza el parámetro ACTIVEATAPOOLS, utilice el mandato COPY ACTIVEATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE. El valor

predeterminado es NO.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50. El valor predeterminado es 1. Si el valor del parámetro DEDUPLICATE es NO, el valor predeterminado de IDENTIFYPROCESS no tiene ningún efecto.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

Ejemplo: definir una agrupación de almacenamiento primaria con una clase de dispositivo 8MMTAPE

Definir una agrupación de almacenamiento primaria que se denomine 8MMPool para la clase de dispositivo 8MMTAPE (con el tipo de dispositivo 8MM) y un tamaño de archivo máximo de 5 MB. Almacenar los archivos de más de 5 MB en agrupaciones subordinadas, a partir de POOL1. Se activará la función de proximidad de los archivos de los nodos cliente. Se permitirán hasta 5 volúmenes reutilizables en esta agrupación de almacenamiento.

```
define stgpool 8mmpool 8mmtape maxsize=5m
  nextstgpool=pool1 collocate=node
  maxscratch=5
```

Referencia relacionada:

SET DRMDBBACKUPEXPIREDDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial)

Utilice este mandato para definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
>--POOLtype---COpy--+-----+----->
      '-DESCRiption---descripción-'
      .-ACCess---READWrite-----
>--+-----+----->
      '-ACCess---+READWrite---+'
          +-READOnly---+
          '-UNAVailable-'
      .-COLlocate---No-----
>--+-----+----->
      '-COLlocate---+No-----+'
          +-GRoup-----+
          +-NODE-----+
          '-FILESpace-'
      .-RECLaim---100----- .-RECLAIMProcess---1-----
>--+-----+----->
      '-RECLaim---porcentaje-' '-RECLAIMProcess---number-'
      .-RECLAMATIONType---THRESHold-----
>--+-----+----->
      |                                     (1) |
```

```

'-RECLAMATIONType--++-THRESHold+-----'
          '-SNAPlock--'

.-OFFSITERECLAIMLimit---NOLimit-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-OFFSITERECLAIMLimit---number--'

.-REUsedelay---0----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-REUsedelay---días-' '-OVFLocation---ubicación-'

.-DATAFormat---Native-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     (2) |
'-DATAFormat---Native-----+-----'
          +-NONblock----+
          +-NETAPPDump--+
          +-CELERRADump--+
          '-NDMPDump----'

.-CRCDATA---No----- .-DEDuplicate---No-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-CRCDATA---Yes-+-' '-DEDuplicate---No-----+-'
          '-No--' | (3) |
                  '-Yes-----'

.-IDENTIFYProcess---0-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+<<
|                                     (4) |
'-IDENTIFYProcess---número-----'

```

Notas:

1. El valor RECLAMATIONTYPE=SNAPLOCK sólo es válido para las agrupaciones de almacenamiento definidas en los servidores que están activados para IBM Spectrum Protect para retención de datos. La agrupación de almacenamiento debe estar asignada a una clase de dispositivo FILE y los directorios especificados en la clase de dispositivo deben ser volúmenes NetApp SnapLock.
2. Los valores NETAPPDUMP, CELERRADUMP y NDMPDUMP no son válidos para las agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.
3. Este parámetro sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.
4. Este parámetro sólo está disponible cuando el valor del parámetro DEDUPLICATE es YES.

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de definir. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial a la que se asigna esta agrupación de almacenamiento de copia. Puede especificar cualquier clase de dispositivo definida con el mandato DEFINE DEVCLASS.

POoltype=COpy (Necesario)

Especifica que desea definir una agrupación de almacenamiento de copia.

DESCRiption

Especifica la descripción de la agrupación de almacenamiento de copia. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor acceder a los archivos de la agrupación de almacenamiento de copia. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de almacenamiento de copia.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional. El valor predeterminado es NO.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODe

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

REclaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es de 100, lo cual significa que no se lleva a cabo la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de copia que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos sin caducar del volumen reclamable desde una agrupación de almacenamiento de copia o primaria que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de almacenamiento de copia original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de almacenamiento de copia.

RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento de copia. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de copia de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

RECLAMATIONType

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención utilizando el software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido

para agrupaciones de almacenamiento que se definen en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El mandato DEFINE no se ejecutará correctamente si el parámetro RECLAMATIONTYPE especificado es distinto del valor definido para las agrupaciones de almacenamiento ya definidas para el nombre de clase de dispositivo.

OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, suponga que una agrupación de almacenamiento de copias contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclamarán los tres volúmenes cuando se ejecute la reclamación. Si se especifica un valor de 2, sólo se reclamarán VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclamará VOL1.

MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se ha especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento de copia y la capacidad correspondiente estimada para la agrupación de almacenamiento de copia.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de almacenamiento de copia mientras no se cambie la modalidad de acceso. A continuación, un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes

virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen. Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento de copia seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el mandato. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

DATAFormat

Especifica el formato de datos que debe utilizarse para hacer copia de seguridad de archivos en esta agrupación de almacenamiento y restaurarlos de la misma. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

NATIVE

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

NETAPPDump

Especifica que los datos tienen un formato de vuelco NetApp. No especifique este formato de datos para imágenes de sistema de archivos que se encuentran en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos NetApp utilizando NDMP. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NETAPPDUMP. Puede utilizar el mandato MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

CELERRADump

Especifica que los datos tienen un formato de vuelco EMC Celerra. No especifique este formato de datos para imágenes de sistema de archivos que se encuentran en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos EMC Celerra utilizando NDMP. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=CELERRADUMP. Puede utilizar el mandato MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

NDMPDump

Especifica que los datos tienen un formato de copia de seguridad específico del fabricante del NAS. No especifique este formato de datos para imágenes del sistema de archivos de las que se ha hecho copia de seguridad desde un servidor de archivos NAS que no sea NetApp o EMC Celerra. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NDMPDUMP. Puede utilizar el mandato MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

CRCData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en

YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE. El valor predeterminado es NO.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50.

El valor predeterminado para este parámetro es 0. Los procesos de eliminación de duplicados para una agrupación de almacenamiento de copias no son necesarios si se especifican procesos de eliminación de duplicados para la agrupación de almacenamiento primaria. Si IBM Spectrum Protect analiza un archivo de una agrupación de almacenamiento, IBM Spectrum Protect también analiza el archivo que se encuentra en todas las demás agrupaciones de almacenamiento.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

Ejemplo: definir una agrupación de almacenamiento de copia con una clase de dispositivo DC480.

Definir la agrupación de almacenamiento de copia TAPEPOOL2 en la clase de dispositivo DC480. Se permitirán hasta 50 volúmenes reutilizables en esta agrupación. La reutilización de volúmenes se retardará 45 días.

```
define stgpool tapepool2 dc480 pooltype=copy
maxscratch=50 reusedelay=45
```

Referencia relacionada:

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

DEFINE STGPOOL (Definir una agrupación de datos activos asignada a dispositivos de acceso secuencial)

Utilice este mandato para definir una agrupación de almacenamiento de datos asignada a dispositivos de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
>--POOLtype-----ACTIVEdata--+-+-----+----->
      '-DESCRiption-----descripci3n-'
      .-ACCess-----READWrite-----
>+-----+-----+-----+-----+----->
      '-ACCess-----+READWrite-----+'
          +-READOnly-----+
          '-UNAVailable-'
      .-COLlocate-----No-----
>+-----+-----+-----+-----+----->
      '-COLlocate-----+No-----+'
          +-GRoup-----+
          +-NODE-----+
          '-Filespace-'
      .-RECLaim-----60----- .-RECLAIMPRocess-----1-----
>+-----+-----+-----+-----+----->
      '-RECLaim-----porcentaje-' '-RECLAIMPRocess-----number-'
      .-RECLAMATIOnType-----THRESHold-----
>+-----+-----+-----+-----+----->
      |                                     (1) |
      '-RECLAMATIOnType-----+THRESHold+-----+'
          '-SNAPlock--'
      .-OFFSITERECLAIMLimit-----NOLimit-
>+-----+-----+-----+-----+----->
      '-OFFSITERECLAIMLimit-----number--'
      .-REUsedelay-----0-----
>+-----+-----+-----+-----+----->
      '-REUsedelay-----días-' '-OVFLocation-----ubicaci3n-'
      .-DATAFormat-----NATIVE----- .-CRCData-----No-----
>+-----+-----+-----+-----+----->
      '-DATAFormat-----+NATIVE-----+' '-CRCData-----+Yes+-'
          '-NONblock-'                    '-No--'
      .-DEDUPlicate-----No-----
>+-----+-----+-----+-----+----->
      '-DEDUPlicate-----+No-----+'
          |           (2) |
          '-Yes-----'
      .-IDENTIFYPRocess-----0-----
>+-----+-----+-----+-----+-----><
      |                                     (3) |
      '-IDENTIFYPRocess-----número-----'
```

Notas:

1. El valor RECLAMATIONTYPE=SNAPLOCK sólo es válido para las agrupaciones de almacenamiento definidas en los servidores que están activados para IBM Spectrum Protect para retención de datos. La agrupación de almacenamiento debe estar asignada a una clase de dispositivo FILE y los directorios especificados en la clase de dispositivo deben ser volúmenes NetApp SnapLock.
2. Este parámetro sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.
3. Este parámetro sólo está disponible cuando el valor del parámetro DEDUPLICATE es YES.

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de definir. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial a la que se asigna esta agrupación de datos activos. Puede especificar cualquier clase de dispositivo definida con el mandato DEFINE DEVCLASS.

POOLtype=ACTIVEdata (Necesario)

Especifica que desea definir una agrupación de datos activos.

DESCRIPTION

Especifica una descripción de la agrupación de datos activos. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCESS

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, reclamación) pueden acceder a los archivos de la agrupación de datos activos. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

READWRITE

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de datos activos.

READONLY

Especifica que los nodos cliente pueden leer sólo los archivos que están almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

UNAVAILABLE

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

COLLOCATE

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional. El valor predeterminado es NO.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GROUP

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo

nodo también pueden distribuirse en varias cintas asociadas con un grupo.

- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

RECLAIM

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación produce que el espacio fragmentado y el espacio que ocupan los archivos de copia de seguridad inactivos en los volúmenes pueda volver a utilizarse traspasando los restantes archivos no caducados y los archivos de copia de seguridad activos desde un volumen hasta otro volumen. Esta acción hace que el volumen original esté disponible para su reutilización. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es 60.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de datos activos que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación primaria o de datos activos que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de datos activos original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de datos activos.

RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de datos activos. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de datos activos de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

RECLAMATIONType

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención utilizando el software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido para agrupaciones de almacenamiento que se definen en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El mandato DEFINE no se ejecutará correctamente si el parámetro RECLAMATIONTYPE especificado es distinto del valor definido para las agrupaciones de almacenamiento ya definidas para el nombre de clase de dispositivo.

OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, imaginemos que una agrupación de datos activos contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no

especifica un valor para este parámetro OFFSITERECLAIMLIMIT, se reclaman los tres volúmenes cuando se ejecute la reclamación. Si especifica un valor de 2, sólo se reclaman VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclama VOL1.

MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se especifica para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de datos activos y la capacidad correspondiente estimada para la agrupación de datos activos.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de datos activos mientras no se cambie la modalidad de acceso. A continuación, un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de datos activos seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el mandato. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

DATAFormat

Especifica el formato de datos que ha de utilizarse para copiar archivos en esta agrupación de almacenamiento y restaurar los archivos de esta agrupación de almacenamiento. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

NATive

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. El valor predeterminado es NO.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50.

El valor predeterminado para este parámetro es 0. Los procesos de eliminación de duplicados para una agrupación de almacenamiento de copias no son necesarios si se especifican procesos de eliminación de duplicados para la agrupación de almacenamiento primaria. Si IBM Spectrum Protect analiza un archivo de una agrupación de almacenamiento, IBM Spectrum Protect también analiza el archivo que se encuentra en todas las demás agrupaciones de almacenamiento.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

Ejemplo: definir una agrupación de datos activos con una clase de dispositivo DC500

Definir una agrupación de datos activos, TAPEPOOL2, para la clase de dispositivo DC500. Se permitirán hasta 50 volúmenes reutilizables en esta agrupación. La reutilización de volúmenes se retardará 45 días.

```
define stgpool tapepool3 dc500 pooltype=activedata
maxscratch=50 reusedelay=45
```

Referencia relacionada:

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para definir uno o varios directorios en una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.

Consejo: Después de definir una agrupación de almacenamiento de contenedor en la nube, cree uno o varios directorios que se utilicen para el almacenamiento local. Temporalmente puede almacenar los datos en el almacenamiento local durante la ingesta de datos, y antes de mover los datos a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado. Para obtener más información, consulte el apartado Optimización del rendimiento para el almacenamiento de objetos en la nube.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGPOOLDIRectory--nombre_agrupación-----nombre_directorio+----><
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Este parámetro es obligatorio.

nombre_directorio (Obligatorio)

Especifica el directorio que debe definirse en la agrupación de almacenamiento. Este parámetro es necesario. Puede especificar más de un nombre de directorio separando cada nombre con una coma y sin espacios intercalados.

Si utiliza el cliente administrativo y el nombre de directorio contiene una coma o una barra inclinada invertida ("\"), especifique el nombre entre comillas.

Ejemplo: Definición de un directorio de agrupación de almacenamiento

Defina un directorio de agrupación de almacenamiento que se denomine DIR1 utilizando una agrupación de almacenamiento de contenedores de directorios que se denomine POOL1.

 Sistemas operativos AIX  Sistemas operativos Linux

```
define stgpooldirectory pool1 /storage/dir1
```

 Sistemas operativos Windows

```
define stgpooldirectory pool1 c:\storage\dir1
```

Ejemplo: Definir varios directorios de agrupaciones de almacenamiento

Defina directorios de agrupaciones de almacenamiento que se denominen DIR1 y DIR2 utilizando una agrupación de almacenamiento de contenedores de directorios que se denomine POOL1.

 Sistemas operativos AIX  Sistemas operativos Linux

```
define stgpooldirectory pool1 /storage/dir1,/storage/dir2
```

 Sistemas operativos Windows

```
define stgpooldirectory pool1 e:\storage\dir1,f:\storage\dir2
```

Ejemplo: definir un almacenamiento local para una agrupación de almacenamiento de contenedor de nubes

Cree un directorio de agrupación de almacenamiento denominado DIR3 en una agrupación de almacenamiento de contenedor de nubes que se llame CLOUDLOCALDISK1.

 Sistemas operativos AIX  Sistemas operativos Linux

```
define stgpooldirectory cloudlocaldisk1 /storage/dir3
```

 Sistemas operativos Windows

```
define stgpooldirectory cloudlocaldisk1 c:\storage\dir3
```

Tabla 1. Mandatos relacionados con DEFINE STGPOOLDIRECTORY

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

DEFINE STGRULE (Definir una regla de almacenamiento para agrupaciones de almacenamiento)

Utilice este mandato para definir una regla de almacenamiento para una o más agrupaciones de almacenamiento. La regla de almacenamiento planifica niveles entre las agrupaciones de almacenamiento de contenedores. Puede definir una o más reglas de almacenamiento para una misma agrupación de almacenamiento de contenedores de destino.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine STGRULE--nombre_regla--agrup_almac_destino----->
>---ACTiontype---Nivel----->
. ,-----
v |
>-----SRCpools---agrupación_origen+----->
. -TIERDelay---30----- . -MAXPRocess---8-----
>+-----+-----+-----+----->
'-TIERDelay---retardo-' '-MAXPRocess---número-'
. -DURation---NOLimit-. . -STARTTime---hora_actual-.
>+-----+-----+-----+----->
'-DURation---minutos-' '-STARTTime---hora-----'
. -ACTIVE---Yes-----
>+-----+-----+-----+-----<
'-ACTIVE---+No--+-' '-DESCRiption---descripción-'
'-Yes-'
```

Parámetros

nombre_regla(Necesario)

Especifica el nombre de la regla de almacenamiento. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

agrupación_destino(Necesario)

Especifica el nombre de la agrupación de almacenamiento de contenedores en la nube de destino.

ACTiontype=Tier (Necesario)

Especifica que la regla nivela objetos de la agrupación de almacenamiento origen a la agrupación de almacenamiento de destino.

Puede utilizar niveles para reducir los costes de almacenamiento moviendo los datos a una agrupación de almacenamiento de contenedores en la nube.

SRCPools (Necesario)

Especifica el nombre del directorio origen de agrupaciones de almacenamiento de contenedores. Si especifica una agrupación como la fuente de una regla de almacenamiento, no puede especificar la misma agrupación como origen de otra regla de

almacenamiento. Para especificar varias agrupaciones de almacenamiento, separe los nombres con comas sin espacios intercalados. Debe especificar este parámetro si también especifica el parámetro ACTIONTYPE=TIER.

TIERDelay

Especifica el número de días que esperar antes de la regla de almacenamiento nivele los objetos a la siguiente agrupación de almacenamiento. El valor predeterminado es 30 días. Puede especificar un entero en el rango 0 – 9999. El valor del parámetro se aplica a todos los archivos de la agrupación de almacenamiento.

MAXProcess

Especifica el número máximo de procesos paralelos para completar la regla de almacenamiento para cada agrupación de almacenamiento de origen que se ha especificado. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 8. Por ejemplo, si tiene 4 agrupaciones de almacenamiento de origen y especifica el valor predeterminado para este parámetro, se inician 32 procesos.

DURATION

Especifica el número máximo de minutos que se ejecutará la regla de almacenamiento antes de que se cancele automáticamente. Puede especificar un número comprendido entre 60 y 1440. El valor predeterminado es ilimitado. Si no especifica un valor, o si especifica un valor de NOLimit, la regla de almacenamiento se ejecuta hasta que se completa. Este parámetro es opcional.

STARTTime

Especifica el tiempo para el inicio de la ventana en la que la regla de almacenamiento se procesa por primera vez. El valor predeterminado es la hora actual. Este parámetro es opcional. La regla de almacenamiento se ejecuta diariamente dentro de 5 minutos después del tiempo especificado.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	23:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más el número especificado de horas y minutos.	NOW+02:00 o +02:00
NOW-HH:MM o -HH:MM	La hora actual menos el número especificado de horas y minutos.	NOW-02:00 o -02:00

ACTIVE

Especifica si se produce el proceso de la regla de almacenamiento. Este parámetro es opcional. El valor predeterminado es YES. Son posibles los siguientes valores:

No

Especifica que la regla de almacenamiento está inactiva. La regla de almacenamiento no se procesa en el momento planificado.

Yes

Especifica que la regla de almacenamiento está activa. La regla de almacenamiento se procesa en el momento planificado.

DESCRIPTION

Especifica una descripción de la regla de almacenamiento. Este parámetro es opcional.

Definir una regla de almacenamiento

Definir una regla de almacenamiento que se denomina tieraction para mover datos desde las agrupaciones de almacenamiento de contenedores de directorio origen dirpool1 y dirpool2 a la agrupación de almacenamiento de contenedor en la nube cloudpool1. Especificar las 03:00 como hora de inicio y utilizar un máximo de 10 procesos para una regla de almacenamiento de nivel:

```
define stgrule tieraction cloudpool1 srcpools=dirpool1,dirpool2
actiontype=tier maxprocess=10 starttime=03:00:00
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE STGRULE

Mandato	Descripción
DELETE STGRULE	Suprimir reglas de almacenamiento para las agrupaciones de almacenamiento.
QUERY STGRULE	Visualizar información sobre reglas de almacenamiento.
UPDATE STGRULE	Actualiza una regla de almacenamiento para las agrupaciones de almacenamiento.

DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)

Utilice este mandato en un servidor gestionado para suscribir dicho servidor a un perfil.

Cuando un servidor se suscribe a su primer perfil, también se crea una suscripción al perfil predeterminado (si existe) del gestor de configuración. Entonces, el servidor establece contacto periódicamente para actualizar la configuración.

Restricciones:

1. Un servidor no se puede suscribir a perfiles de más de un gestor de configuración.
2. Si un servidor se suscribe a un perfil con un objeto asociado que ya está definido en el servidor, la definición local se sustituye por la definición del gestor de configuración. Por ejemplo, si un servidor tiene una planificación de administración denominada WEEKLY_BACKUP, y después se suscribe en un perfil que también tiene una planificación de administración denominada WEEKLY_BACKUP, se sustituirá la definición local.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DEFine SUBSCRIPtion--nombre_perfil----->
>--+-----+-----<
  '-SERVer----nombre_servidor-'
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el nombre del perfil en el que se suscribe el servidor.

SERVer

Especifica el nombre del gestor de configuración del que se obtiene la información de configuración. Este parámetro es necesario si el servidor gestionado no tiene una suscripción como mínimo. Si el servidor gestionado tiene una suscripción, puede omitir este parámetro y se tomará el gestor de configuración como valor predeterminado para dicha suscripción.

Ejemplo: definir una suscripción de perfil

Suscribir un perfil denominado BETA que reside en un gestor de configuración denominado TOM.

```
define subscription beta server=tom
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE SUBSCRIPTION

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.

Mandato	Descripción
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGREFRESH	Especifica un intervalo de tiempo para que los servidores gestionados entren en contacto con los gestores de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)

Utilice este mandato para definir una correlación de espacios de archivos virtuales.

En las operaciones de datos NAS BACKUP NODE y RESTORE NODE, pueden utilizarse nombres de espacios de archivos virtuales similares a un nombre del sistema de archivos. Consulte la documentación sobre el dispositivo NAS para obtener orientación acerca de cómo especificar los parámetros de este mandato.

Nota: El nodo NAS debe tener una definición de transportador de datos asociada porque, cuando el servidor de IBM Spectrum Protect actualiza una correlación de espacios de archivos virtuales, el servidor intenta ponerse en contacto con el dispositivo NAS para validar el sistema de archivos virtuales y el nombre del sistema de archivos.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

Sintaxis

```
>>-DEFine VIRTUALFSmapping  -nombre_nodo----->
>--nombre_espacio_archivos_virtual--nombre_sistema_archivos----->
      .-NAMeType----SERVER-----
>--ruta-+-----+-----+-----><
      '-NAMeType----+-SERVER-----+'
              '-HEXadecimal-'
```

Parámetros

nombre_nodo (Necesario)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre_espacio_archivos_virtual (Obligatorio)

Especifica el nombre que hace referencia a esta definición de espacio de archivos virtual. El nombre de espacio de archivos virtual es sensible a las mayúsculas y minúsculas y el primer carácter debe ser una barra inclinada /. La longitud del nombre no puede ser mayor que 64 caracteres, incluida la barra inclinada necesaria. Los nombres de los espacios de archivos virtuales están limitados al mismo juego de caracteres establecido para el resto de objetos del servidor, excepto el carácter de barra inclinada /, que también está permitido.

El nombre del espacio de archivos virtual no puede ser idéntico a ningún sistema de archivos en el nodo NAS. Al seleccionar un nombre de espacio de archivos virtual, tenga en cuenta las restricciones siguientes:

- Si se crea un sistema de archivos en el dispositivo NAS con el mismo nombre que un sistema de archivos virtual, se producirá un conflicto de nombres en el servidor al realizarse la copia de seguridad del nuevo espacio de archivos. Utilice

una cadena de caracteres para el nombre de espacio de archivos virtual que es poco probable que se utilice en el futuro como un nombre de sistema de archivos real en el dispositivo NAS.

Por ejemplo: un usuario sigue un convenio de denominación para crear espacios de archivos en un dispositivo NAS con los nombres de formato /vol1, /vol2, /vol3. El usuario define un espacio de archivos virtual en el servidor con el nombre /vol9. Si continúa utilizando los mismos convenios de denominación, es muy probable que el nombre del espacio de archivos virtual entre en conflicto con un nombre de espacio de archivos real en algún momento del futuro.

- Durante las operaciones de copia de seguridad y restauración, el servidor verifica que no se produzca ningún conflicto de nombres antes de iniciar la operación.
- El nombre del espacio de archivos virtual aparecerá como un espacio de archivos en la salida del mandato QUERY FILESPACE, así como en los paneles de copia de seguridad y restauración del cliente web de IBM Spectrum Protect. Por lo tanto, debe considerar la posibilidad de seleccionar un nombre que identifique sin ningún tipo de ambigüedad este objeto como una ruta de directorio en el dispositivo NAS.

nombre_sistema_archivos (Obligatorio)

Especifica el nombre del sistema de archivos en el que se encuentra la ruta. El nombre del sistema de archivos debe existir en el nodo NAS especificado. El nombre del sistema de archivos no puede contener caracteres comodín.

ruta (Obligatorio)

Especifica la ruta de la raíz del sistema de archivos al directorio. La ruta sólo puede hacer referencia a un directorio. La longitud máxima de la ruta es de 1024 caracteres. El nombre de ruta es sensible a las mayúsculas y minúsculas.

NAMETYPE

Especifica la forma en la que el servidor debe interpretar el nombre de ruta especificado. Este parámetro es útil cuando una ruta contiene caracteres que no forman parte de la página de códigos en que se ejecuta el servidor. El valor predeterminado es SERVER.

Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar el nombre de ruta.

HEXadecimal

El servidor interpreta el nombre de ruta que ha entrado como la representación hexadecimal de la ruta. Esta opción debe utilizarse cuando una ruta contenga caracteres que no se pueden entrar. Esto podría ocurrir si el sistema de archivos NAS se establece en un idioma diferente de aquél en que se ejecuta el servidor.

Ejemplo: definir una correlación de espacios de archivos virtuales

Definir el nombre de correlación de espacios de archivos virtuales /mikeshomedir para la ruta /home/mike en el sistema de archivos /vol/vol1 del nodo NAS denominado NAS1.

```
define virtualfsmapping nas1 /mikeshomedir /vol/vol1 /home/mike
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DEFINE VIRTUALFSMAPPING



Mandato	Descripción
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)

Utilice este mandato para asignar un volumen de acceso secuencial o aleatorio a una agrupación de almacenamiento.

Cuando se defina un volumen de agrupación de almacenamiento de acceso aleatorio (DISK) o un volumen de agrupación de almacenamiento de acceso secuencial asociado a una clase de dispositivo FILE, puede utilizar el servidor para que éste cree el volumen antes de que se asigne. O bien puede utilizar los desencadenantes de espacio para crear volúmenes preasignados cuando se hayan excedido los umbrales de utilización de espacio predeterminados. Para obtener detalles sobre los desencadenantes de espacio,

consulte el apartado DEFINE SPACETRIGGER (Definir desencadenante de espacio). Para obtener volúmenes asociados con clases de dispositivos diferentes a DISK o tipos de dispositivos diferentes a FILE, puede utilizar el mandato DEFINE VOLUME para asignar un volumen ya creado a una agrupación de almacenamiento.


 Sistemas operativos AIX  Sistemas operativos Linux Cuando se utiliza una clase de dispositivo FILE para el almacenamiento gestionado por el servidor de medios de z/OS, no es necesario formatear o definir volúmenes. Si define un volumen para este tipo de clase de dispositivo FILE utilizando el mandato DEFINE VOLUME, el servidor de medios de z/OS no asigna espacio para el volumen hasta que se abra el volumen para su primer uso.


Atención: Los volúmenes para el servidor de medios de z/OS que se crean mediante el mandato DEFINE VOLUME permanecen llenos físicamente o asignados después de que el servidor vacía el volumen, por ejemplo, después de la caducidad o la reclamación. Para los volúmenes FILE, el espacio DASD no se cede al sistema cuando se vacía el volumen. Si una agrupación de almacenamiento requiere un volumen de relleno o vacío, se puede utilizar el volumen FILE. En comparación, los volúmenes de cinta que se vacían lógicamente son igual que si estuvieran vacíos físicamente. Los volúmenes de cinta y FILE permanecen definidos en el servidor. En comparación, los volúmenes reutilizables, incluido el almacenamiento físico que se asigna para los volúmenes de archivo reutilizables, se devuelven al sistema cuando se vacían.

Para crear espacio en las agrupaciones de almacenamiento de acceso secuencial, puede definir volúmenes o permitir al servidor solicitar volúmenes reutilizables según sea necesario, tal y como especifica el parámetro MAXSCRATCH para la agrupación de almacenamiento. En el caso de agrupaciones de almacenamiento asociadas a la clase de dispositivo FILE, el servidor puede crear volúmenes privados según sea necesario por medio de los desencadenantes de espacio de la agrupación de almacenamiento. En el caso de agrupaciones de almacenamiento DISK, el mecanismo reutilizable no está disponible. No obstante, puede crear espacio si crea volúmenes y, a continuación, los define en el servidor. O bien, puede hacer que el servidor cree los volúmenes que utilizan desencadenantes de espacio de agrupación de almacenamiento.


El servidor no valida la existencia de un nombre de volumen al definir un volumen en una agrupación de almacenamiento asociada a una biblioteca. El volumen definido tiene una capacidad estimada "0" hasta que se graban datos en él.

Atención: El tamaño de un volumen de agrupación de almacenamiento no se puede cambiar después de que se ha definido en el servidor.

 Sistemas operativos AIX Si cambia el tamaño de los volúmenes de IBM Spectrum Protect ampliando los volúmenes lógicos con formato RAW mediante SMIT o modificando el tamaño de los archivos de los volúmenes con mandatos o programas de utilidad de sistema operativo, es posible que el servidor no se inicialice correctamente y se pierdan datos.

 Sistemas operativos Windows Si cambia el tamaño de los volúmenes modificando el tamaño de los archivos de los volúmenes con mandatos o programas de utilidad de sistema operativo, es posible que el servidor no se inicialice correctamente y se pierdan datos.

Restricciones:

- Este mandato no puede utilizarse para definir volúmenes en agrupaciones de almacenamiento con el valor de parámetro RECLAMATIONTYPE=SNAPLOCK. Los volúmenes de este tipo de agrupación de almacenamiento se han asignado utilizando el parámetro MAXSCRATCH en la definición de agrupación de almacenamiento.
- No puede definir volúmenes de una agrupación de almacenamiento definida con la clase de dispositivo CENTERA.
-  Sistemas operativos Linux No se pueden utilizar volúmenes lógicos RAW para los volúmenes de agrupación de almacenamiento.

Los archivos físicos que están asignado al mandato DEFINE VOLUME no se eliminan de un espacio de archivos si emite el mandato DELETE VOLUME.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento a la que se asigna el volumen.

Sintaxis

```
>>>DEFINE Volume--nombre_agrupación--nombre_volumen----->
      .-ACCess----READWrite-----
>---+-----+-----+-----+----->
      '-ACCess----+READWrite----+'
          +-READOnly----+
          +-UNAVailable+
          |         (1) |
          '-Offsite-----'
```


Requisitos de nombre de volumen	Ejemplo
<p>El nombre del archivo que contendrá los datos del volumen, con el nombre de ruta totalmente calificado o con el nombre de ruta relativo al directorio identificado en el parámetro DIRECTORY para la clase de dispositivo.</p> <p> Si un nombre contiene espacios en blanco intercalados, signos de igual u otros caracteres especiales, delimite la lista con comillas.</p> <p>Coloque los volúmenes FILE en uno de los directorios que se especifican con el parámetro DIRECTORY del mandato DEFINE DEVCLASS. De lo contrario, es posible que los agentes de almacenamiento no tengan acceso a los volúmenes. Para obtener detalles, consulte el apartado DEFINE PATH (Definir una ruta).</p>	<p> Sistemas operativos AIX Sistemas operativos Linux</p> <p>/data/fpool01.dsm</p> <p> Sistemas operativos Windows</p> <p>"f:\data storage\fpool01.dsm"</p>

Sistemas operativos AIX Sistemas operativos Linux

Tabla 3. servidor de medios de z/OS: requisitos de nombre de volumen para FILE

Requisitos de nombre de volumen	Ejemplo
<p>Para los volúmenes FILE utilizados con el servidor de servidor de medios de z/OS, especifique un nombre de conjunto de datos. El nombre del conjunto de datos puede constar de uno o más calificadores delimitados por un punto. Los calificadores pueden contener un máximo de 8 caracteres. La longitud máxima del nombre del conjunto de datos es de 44 caracteres. La primera letra de cada calificador debe ser un carácter alfabético o nacional (@#\$), seguido de caracteres alfabéticos, nacionales, numéricos o guiones.</p> <p>Para asignar el conjunto de datos lineal VSAM asociado cuando se presenta el volumen en el sistema z/OS, el calificador de alto nivel (HLQ) se suele filtrar mediante rutinas de selección automática de clases específicas en las restricciones de política de SMS en el sistema donde se ejecuta el servidor de medios de z/OS.</p> <p>El comportamiento del calificador de alto nivel es similar al del nombre PREFIX en una solicitud reutilizable. El calificador de alto nivel suele utilizarlo DFSMS para afectar los atributos de asignación, como Extended Addressability para los conjuntos de datos que se espera que se amplíen cuando el espacio que ya está asignado al volumen de archivo se ha agotado.</p> <p>Si no existe el conjunto de datos, el servidor lo crea cuando se utiliza el volumen para una operación de almacenamiento de IBM Spectrum Protect específica. El conjunto de datos no se crea cuando se define el volumen. Se puede producir una pérdida de datos al definir volúmenes porque el servidor de medios de z/OS reutiliza el volumen o el conjunto de datos lineal VSAM si existe en el momento del tiempo de asignación. Importante: Para permitir que el servidor genere nombres de volumen, considere utilizar volúmenes reutilizables.</p>	<p> Sistemas operativos AIX Sistemas operativos Linux</p> <p>SERVER1.BFS.POOL3.VOLA</p>

Tabla 4. Requisitos de nombre de volumen para cinta

Requisitos de nombre de volumen	Ejemplo
<p>Uso de 1 a 32 caracteres alfanuméricos.</p> <p>El nombre de volumen no puede contener espacios en blanco intercalados ni signos de igual.</p>	<p>DSMT01</p>

Tabla 5. servidor de medios de z/OS: requisitos de nombre de volumen para cinta

Requisitos de nombre de volumen	Ejemplo
<p>Para los cartuchos de cinta, especifique un nombre de volumen de cinta con 1 a 6 caracteres alfanuméricos. El servidor convierte en mayúsculas los nombres de volumen de cinta.</p> <p>El nombre de volumen no puede contener espacios en blanco intercalados ni signos de igual.</p> <p>Los volúmenes que el servidor utiliza para cualquier fin debe tener un nombre exclusivo. Este requisito es válido para todos los volúmenes, tanto si se utilizan para las agrupaciones de almacenamiento como si se emplean para operaciones como una copia de seguridad o exportación de base de datos. El requisito se aplica también a los volúmenes que residen en distintas bibliotecas de medios de z/OS pero que utiliza el mismo servidor.</p>	DSMT01

Tabla 6. Requisitos de nombre de volumen para REMOVABLEFILE

Requisitos de nombre de volumen	Ejemplo
<p>1–6 caracteres alfanuméricos</p> <p>El servidor convierte en mayúsculas los nombres de volumen.</p>	DSM01

ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor (como, por ejemplo, migración) acceder a los archivos del volumen de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Los valores posibles son:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en el volumen.

READOnly

Especifica que los nodos de cliente y los procesos de servidor sólo pueden realizar operaciones de lectura en los archivos almacenados en el volumen.

UNAVailable

Especifica que ni los nodos de cliente ni los procesos de servidor pueden acceder a los archivos almacenados en el volumen.

Si define un volumen de acceso aleatorio como UNAVAILABLE, no podrá activar el volumen.

Si define un volumen de acceso secuencial como UNAVAILABLE, el servidor no intentará acceder al volumen.

OFFsite

Especifica que el volumen está en una ubicación fuera de local desde la que no se puede montar. Este valor sólo se puede especificar para los volúmenes de agrupaciones de almacenamiento de copia o de datos activos.

Utilice este valor para poder localizar los volúmenes de las ubicaciones de fuera del local. El servidor trata los volúmenes que están designados como fuera del local de forma diferente:

- El servidor no genera peticiones de montaje para los volúmenes designados como fuera de local.
- El servidor reclama o traspasa datos de los volúmenes fuera de local recuperando los archivos de otras agrupaciones de almacenamiento.
- El servidor no suprime automáticamente de una agrupación de almacenamiento de copia o de datos activos los volúmenes reutilizables de fuera de local vacíos.

LOcation

Especifica la ubicación del volumen. Este parámetro es opcional. Este parámetro únicamente puede especificarse para los volúmenes de agrupaciones de almacenamiento de acceso secuencial. La información de ubicación puede tener una longitud máxima de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco.

FormaTsize

Especifica el tamaño del volumen de acceso aleatorio o volumen FILE que se crea y formatea en un paso. El valor se especifica en megabytes. El tamaño máximo es de 8.000.000 MB (8 terabytes). Este parámetro es necesario si se da alguna de las

condiciones siguientes:

- Se especifica un solo volumen FILE o DISK que se crea y formatea en un paso.
- El valor del parámetro NUMBEROFVOLUMES es superior a 1 y se están creando volúmenes DISK.
- El valor del parámetro NUMBEROFVOLUMES es mayor que 1 y el valor del parámetro FORMATSIZES es igual o menor que el parámetro MAXCAPACITY del mandato DEFINE DEVCLASS.

Si está asignando volúmenes en un servidor de medios de z/OS, este parámetro no es válido.

Para un volumen FILE, debe especificar un valor menor o igual que el valor del parámetro MAXCAPACITY de la clase de dispositivo asociada a la agrupación de almacenamiento.

No puede utilizar este parámetro para varios volúmenes predefinidos. A menos que se especifique `WAIT=YES`, la operación se realizará como un proceso en segundo plano.

Numberofvolumes

Especifica el número de volúmenes que se crean y formatean en un paso. Este parámetro sólo se aplica a agrupaciones de almacenamiento con clases de dispositivo DISK o FILE. Este parámetro es opcional. El valor predeterminado es 1. Si especifica un valor mayor que 1, también debe especificar un valor para el parámetro FORMATSIZES. Especifique un número de 1 a 256.

Si está asignando volúmenes en un servidor de medios de z/OS, el único valor que admite este parámetro es el valor predeterminado de 1.

Si el valor del parámetro NUMBEROFVOLUMES es mayor que 1, se agregará un sufijo numérico al nombre del volumen que ha especificado para crear cada nombre ,por ejemplo, tivivol001 y tivivol002. Asegúrese de elegir un nombre de volumen para crear un nombre de archivo válido para el sistema de archivos de destino cuando se agrega el sufijo.

Importante: Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para obtener más información, consulte el apartado DEFINE PATH (Definir una ruta).

Wait

Especifica si se realiza una operación de creación y formato de volumen de modo subordinado o en primer plano. Este parámetro es opcional. No se tiene en cuenta excepto si se especifica también el parámetro FORMATSIZES.






No

Especifica que se realiza una operación de creación y formato de volumen de modo subordinado. El valor NO es el valor predeterminado cuando se especifica también un tamaño de formato.

Yes

Especifica que la operación de creación y formateo de un volumen se ejecuta en primer plano.
Recuerde: No se puede especificar `WAIT=YES` desde la consola del servidor.

Ejemplo: utilizar un proceso subordinado para definir un nuevo volumen de 100 MB para una agrupación de almacenamiento de disco

Crear un volumen de 100 MB en la agrupación de almacenamiento de disco denominada BACKUPPOOL.  Sistemas operativos AIX  Sistemas operativos Linux El nombre del volumen es `/var/storage/bf.dsm`.  Sistemas operativos Windows El nombre de volumen es `j:\storage\bf.dsm`. El volumen se creará como proceso subordinado.  Sistemas operativos AIX  Sistemas operativos Linux

```
define volume backuppool  
/var/storage/bf.dsm formatsize=100
```

 Sistemas operativos Windows

```
define volume backuppool j:\storage\bf.dsm formatsize=100
```



Ejemplo: definir un volumen para una agrupación de almacenamiento de disco con acceso de lectura y grabación




La agrupación de almacenamiento denominada POOL1 está asignada a una clase de dispositivo de cinta. Definir el volumen denominado TAPE01 en esta agrupación de almacenamiento, con acceso READWRITE.

```
define volume pool1 tape01 access=readwrite
```


Ejemplo: definir un volumen para una agrupación de almacenamiento de archivo

La agrupación de almacenamiento que se denomina FILEPOOL está asignada a una clase de dispositivo con el tipo de dispositivo FILE.

 Sistemas operativos AIX  Sistemas operativos Linux Definir un volumen que se denomina `filepool_vol01` para esta agrupación de

almacenamiento.  Sistemas operativos Windows Definir un volumen que se denomina fp_vol01.dsm para esta agrupación de almacenamiento.  Sistemas operativos AIX  Sistemas operativos Linux

```
define volume filepool /usr/storage/filepool_vol01
```

 Sistemas operativos Windows

```
define volume filepool j:\storage\fp_vol01.dsm
```

Ejemplo: utilizar un proceso en segundo plano para definir 10 volúmenes para una agrupación de almacenamiento de archivo con una capacidad máxima de 5 GB de clase de dispositivo

Defina 10 volúmenes en una agrupación de almacenamiento secuencia que utiliza una clase de dispositivo FILE. La agrupación de almacenamiento se denomina FILEPOOL. El valor del parámetro MAXCAPACITY para la clase de dispositivo asociada a esta agrupación de almacenamiento es 5 GB. La creación debe realizarse en segundo plano.

```
define volume filepool filevol numberofvolumes=10 formatsize=5000
```

El servidor crea los nombres de volumen filevol001 a filevol010.

Los volúmenes se crean en el directorio o directorios que se han especificado con el parámetro DIRECTORY de la clase de dispositivo que está asociada con la agrupación de archivos de la agrupación de almacenamiento. Si ha especificado varios directorios para la clase de dispositivo, los volúmenes individuales se pueden crear en cualquiera de los directorios de la lista.

Mandatos relacionados

Tabla 7. Mandatos relacionados con DEFINE VOLUME

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

Mandatos DELETE

Utilice los mandatos DELETE para suprimir o eliminar un objeto de IBM Spectrum Protect.

- DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)
- DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)
- DELETE BACKUPSET (Suprimir un juego de copias de seguridad)
- DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)
- DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)
- DELETE COLLOGROUP (Suprimir un grupo de proximidad)
- DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)
- DELETE COPYGROUP (Suprimir un grupo de copias de seguridad o de archivado)
- DELETE DATAMOVER (Suprimir un transportador de datos)
- DELETE DEDUPSTATS (Suprimir las estadísticas de eliminación de duplicados de datos)
- DELETE DEVCLASS (Suprimir una clase de dispositivo)
- DELETE DOMAIN (Suprimir un dominio de políticas)
- DELETE DRIVE (Suprimir una unidad de una biblioteca)
- DELETE EVENT (Suprimir registros de eventos)
- DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)
- DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)
- DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)
- DELETE LIBRARY (Suprimir una biblioteca)
- DELETE MACHINE (Suprimir información de una máquina)
- DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)
- DELETE MGMTCLASS (Suprimir una clase de gestión)

- DELETE NODEGROUP (Suprimir un grupo de nodos)
- DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)
- DELETE PATH (Suprimir una ruta)
- DELETE POLICYSET (Suprimir un juego de políticas)
- DELETE PROFASSOCIATION (Suprimir una asociación de perfil)
- DELETE PROFILE (Suprimir un perfil)
- DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)
- DELETE RECOVERYMEDIA (Suprimir medio de recuperación)
- DELETE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)
- DELETE SCRIPT (Suprimir líneas de mandatos de un script o suprimir todo el script)
- DELETE SERVER (Suprimir una definición de servidor)
- DELETE SERVERGROUP (Suprimir un grupo de servidores)
- DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)
- DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)
- DELETE STGRULE (Suprimir reglas de almacenamiento para agrupaciones de almacenamiento)
- DELETE STGPOOL (Suprimir una agrupación de almacenamiento)
- DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)
- DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)
- DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)
- DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)
- DELETE VOLHISTORY (Suprimir información histórica de volúmenes)
- DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)

Utilice este mandato para suprimir un mensaje de la lista de desencadenantes de alerta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-n-----
      v               |
>>-DELeTe ALERTTrigger-----+---número_mensaje-+-----><

```

Parámetros

número_mensaje (Obligatorio)

Especifica el número de mensajes que desea eliminar de la lista de desencadenantes de alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres. Puede utilizar caracteres comodín para especificar números de mensajes.

Suprimir desencadenante de alerta

Suprima dos números de mensaje que se han designado como alertas, emitiendo el mandato siguiente:

```
delete alerttrigger ANR1067E,ANR1073E
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE ALERTTRIGGER

Mandato	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.

Mandato	Descripción
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)

Utilice este mandato para suprimir la asociación que hay entre un nodo cliente y una planificación de cliente. IBM Spectrum Protect ya no ejecuta la planificación en el nodo cliente.

Si intenta suprimir la asociación entre un cliente y una planificación a la que no está asociado, este mandato no tendrá vigor alguno para dicho cliente.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que pertenece la planificación

Sintaxis

```
>>-DELeTe ASSOCIation--nombre_dominio--nombre_planificación----->
      .-,-----
      v          |
>----nombre_nodo+-----><
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación de la que se deben disociar los clientes.

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente que ya no está asociado a la planificación de cliente. Puede especificar una lista de clientes que dejarán de estar asociados con la planificación especificada. Los elementos de la lista se separan con comas, sin espacios intercalados. También puede utilizar un carácter comodín para especificar un nombre. Todos los clientes coincidentes dejarán de estar asociados con la planificación especificada.

Ejemplo: suprimir una asociación de nodo con una planificación

Para suprimir la asociación del nodo JEFF, asignado al dominio de políticas DOMAIN1, con la planificación WEEKLY_BACKUP, emita el mandato siguiente:

```
delete association domain1 weekly_backup jeff
```

Ejemplo: suprimir una asociación de nodo con una planificación con un comodín para la selección de los nodos

Suprimir la asociación de los clientes seleccionados, asignados al dominio de políticas DOMAIN1, con la planificación WEEKLY_BACKUP para que estos clientes ya no puedan ejecutar esta planificación. Los nodos que dejan de estar asociados con la planificación contienen ABC o XYZ en el nombre de nodo. Emita el mandato:

Especifica el nombre de los nodos cliente o grupos de nodos cuyos datos se incluyen en los volúmenes de juegos de copias de seguridad especificados. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo que especifique pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener caracteres comodín. Si volúmenes de juegos de copias de seguridad contienen juegos de copias de seguridad de varios nodos, cada juego de copias de seguridad cuyo nombre de nodo coincida con uno de los nombres de nodo especificados se suprimirá.

nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a suprimir. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

BEGINDate

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Utilice este parámetro junto con el parámetro BEGINDATE para especificar un rango para la fecha y la hora. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

ENDDate

Especifica la fecha final en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro junto con el parámetro ENDTIME para especificar un rango para la fecha y la hora. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final del rango en que se ha creado el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro junto con el parámetro ENDDATE para especificar un rango para la fecha y la hora. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-02:00 o -02:00.

WHEREDATAType

Especifica que se van a suprimir los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben suprimir. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben suprimir. Este es el valor predeterminado.

FILE

Especifica que se va a suprimir un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen copias de seguridad de archivos y directorios realizadas por el cliente de copia de seguridad/archivado.

IMAGE

Especifica que se va a suprimir un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad/archivado.

WHERERETention

Especifica el valor de retención, especificado en días, asociado a los juegos de copias de seguridad que se van a suprimir. Puede especificar un entero entre el 0 y el 30000. Los valores son:

días

Especifica que los juegos de copias de seguridad que permanecen retenidos durante este número de días, se suprimirán.

NOLimit

Especifica que los juegos de copias de seguridad que permanecen retenidos indefinidamente, se suprimirán.

WHEREDESCRIPTION

Especifica la descripción asociada al juego de copias de seguridad que se va a suprimir. La descripción que especifique puede contener caracteres comodín. Este parámetro es opcional. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Preview

Especifica si se previsualiza la lista de los juegos de copias de seguridad que se van a suprimir, sin suprimir realmente los juegos de copias de seguridad. Este parámetro es opcional. El valor predeterminado es NO. Los valores son:

No

Especifica que los juegos de copias de seguridad se suprimirán.

Yes

Especifica que el servidor visualiza la lista de los juegos de copias de seguridad que se van a suprimir, sin suprimir realmente los juegos de copias de seguridad.

Ejemplo: suprimir un juego de copias de seguridad

Suprimir el juego de copias de seguridad PERS_DATA.3099 que pertenece al nodo cliente JANE. El juego de copias de seguridad se generó el día 19/11/1998 a las 10:30:05 horas, y la descripción es "Documentation Shop".

```
delete backupset pers_data.3099
begindate=11/19/1998 begintime=10:30:05
wheredescription="documentation shop"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE BACKUPSET

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)

Utilice este mandato para suprimir una opción de cliente de un conjunto de opciones.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restringir o privilegio de políticas restringido.

Sintaxis

```
>>-DELeTe CLIENTOpt--nombre_conjunto_opciones--nombre_opción---->
>--+-----+-----<
  '-SEQnumber--==--+número-+-'
    '-ALL----'
```

Parámetros

nombre_conjunto_opciones (Obligatorio)
Especifica el nombre del conjunto de opciones del cliente.

nombre_opción (Obligatorio)

Especifica una opción cliente válida.

SEQnumber

Especifica un número de secuencia cuando se especifica un nombre de opción más de una vez. Este parámetro es opcional. Los valores válidos son:

n

Especifica un número entero igual o mayor que 0.

ALL

Especifica todos los números de secuencia.

Ejemplo: suprimir la opción de formato de fecha

Suprimir la opción de formato de fecha en un conjunto de opciones denominado *ENG*.

```
delete clientopt eng dateformat
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE CLIENTOPT

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)

Utilice este mandato para suprimir un conjunto de opciones de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restringir o privilegio de políticas restringido.

Sintaxis

```
>>-DELeTe CLOptset--nombre_conjunto_opciones----->>
```

Parámetros

nombre_conjunto_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente que se va a suprimir.

Ejemplo: suprimir un conjunto de opciones de cliente

Suprimir el conjunto de opciones de cliente denominado *ENG*.

```
delete cloptset eng
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE CLOPTSET

Mandato	Descripción
---------	-------------

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

DELETE COLLOGROUP (Suprimir un grupo de proximidad)

Utilice este mandato para suprimir un grupo de proximidad. No puede suprimir un grupo de proximidad si incluye algún miembro.

Puede eliminar todos los miembros del grupo de proximidad mediante la emisión del mandato DELETE COLLOCMEMBER con un comodín en el parámetro nombre_nodo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

```
>>-DElete COLLOGroup--nombre_grupo-----><
```

Parámetros

nombre_grupo
Especifica el nombre del grupo de proximidad que desea suprimir.

Ejemplo: suprimir un grupo de proximidad

Suprimir un grupo de proximidad denominado group1.

```
delete collogroup group1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE COLLOGROUP

Mandato	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.

Mandato	Descripción
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOCGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)

Utilice este mandato para suprimir un nodo de cliente o espacio de archivos de un grupo de proximidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

Suprimir un nodo de un grupo de proximidad

```

      .-.,------.
      v          |
>>-DELeTe COLLOCMember--nombre_grupo----nombre_nodo+-----><

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad del que desea suprimir un nodo de cliente.

nombre_nodo

Especifica el nombre del nodo de cliente que desea suprimir del grupo de proximidad. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nodos.

Suprimir un espacio de archivos de un grupo de proximidad de espacio de archivos

```

      .-.,------.
      v          |
>>-DELeTe COLLOCMember--nombre_grupo--nombre_nodo----->
      .-.,------.
      v          |
>--FIlespace-----nombre_espacio_archivos+----->
      .-NAMEType----SERVER-----
>+-----+-----+-----+----->
  '-NAMEType----+-SERVER--+-'
      +-UNICODE-+
      '-FSID----'
      .-CODEType----BOTH-----
>+-----+-----+-----+-----><
  '-CODEType----+-BOTH-----+-'
      +-UNICODE----+
      '-NONUNICODE-'

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad del que desea suprimir un espacio de archivos.

nombre_nodo

Especifica el nodo de cliente donde se encuentra el espacio de archivos.

Filespace

Especifica el *nombre_espacio_archivos* del nodo de cliente que desea suprimir del grupo de proximidad. Puede especificar uno o más nombres de espacio de archivos que se encuentren en un nodo de cliente específico. Si especifica varios nombres de espacio de archivos, sepárelos con comas, no utilice espacios intercalados. También puede utilizar caracteres comodín al especificar varios nombres de espacio de archivos.

NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Un cliente de copia de seguridad/archivado con soporte de Unicode solamente está disponible para Windows, Macintosh OS 9, Macintosh OS X y NetWare. Utilice este parámetro cuando especifique un nombre de espacio de archivos que no sea un único comodín. Puede especificar un nombre de espacio de archivos cualificado al completo que no contenga un comodín. O bien puede especificar un nombre de espacio de archivos parcialmente cualificado, que puede tener un comodín, pero debe contener otros caracteres. El valor predeterminado es SERVER. Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen realmente los nombres y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos por sus ID de espacio de archivos (FSID).

CODETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro solamente cuando especifique un único carácter comodín para el nombre de espacio de archivos. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Los valores siguientes están disponibles:

BOTH

Incluir los espacios de archivos independientemente del tipo de página de códigos.

UNICODE

Incluir solo espacios de archivos que están en Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en Unicode.

Suprimir miembros de grupo de proximidad

Suprimir dos nodos, NODE1 y NODE2, de un grupo de proximidad, GROUP1.

```
delete collocmember group1 node1,node2
```

Suprimir un espacio de archivos de un grupo de proximidad de espacio de archivos

Emita el mandato siguiente para suprimir el espacio de archivos *cap_27400* del grupo de proximidad *collgrp_2* en el nodo *hp_4483*:

```
delete collocmember collgrp_2 hp_4483 filesystem=cap_27400
```

Suprimir un miembro de grupo de proximidad de espacio de archivos de un nodo que utiliza Unicode

Si el espacio de archivos se encuentra en un nodo que utiliza Unicode, puede especificarlo en el mandato. Emita el mandato siguiente para suprimir el espacio de archivos *cap_257* del grupo de proximidad *collgrp_3* del nodo *win_4687*:

```
delete collocmember collgrp_3 win_4687 filesystem=cap_257 codetype=unicode
```

Suprimir un espacio de archivos con un nombre parcial designado

Si el espacio de archivos tiene un nombre parcial, puede utilizar un comodín para suprimirlo. Emita el mandato siguiente para suprimir el espacio de archivos *cap_* del grupo de proximidad *collgrp_4* del nodo *win_4687*:

```
delete collocmember collgrp_4 win_4687 filesystem=cap_* codetype=unicode
```


Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el grupo de copia.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas al que pertenece el grupo de copia.

nom_clase (Necesario)

Especifica la clase de gestión a la que pertenece el grupo de copia.

STANDARD

Especifica el grupo de copias, que siempre es STANDARD. Este parámetro es opcional. El valor predeterminado es STANDARD.

Type

Especifica el tipo del grupo de copia que se va a suprimir. Este parámetro es opcional. El valor predeterminado es BACKUP. Los valores posibles son:

Backup

Especifica que se suprime el grupo de copia de seguridad.

Archive

Especifica que se suprime el grupo de copia archivada.

Ejemplo: suprimir un grupo de copias de seguridad

Suprimir el grupo de copia de seguridad de la clase de gestión ACTIVEFILES que está en el juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS.

```
delete copygroup employee_records  
vacation activefiles
```

Ejemplo: suprimir un grupo de copias archivadas

Suprimir el grupo de copia archivada de la clase de gestión MCLASS1 que está en el juego de políticas SUMMER del dominio de políticas PROG1.

```
delete copygroup prog1 summer mclass1 type=archive
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE COPYGROUP

Mandato	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

DELETE DATAMOVER (Suprimir un transportador de datos)

Utilice este mandato para suprimir un transportador de datos. No es posible suprimir un transportador de datos si hay rutas definidas en este transportador de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELeTe DATAMover--nombre_transportador_datos-----><
```

Parámetros

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que se incluye en las estadísticas de deduplicación de datos. Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el mandato falla.

Restricción: Sólo puede especificar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de nube.

nombre_nodo

Especifica el nombre del nodo de cliente que se notifica en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Si no especifica un valor para este parámetro, se visualizarán todos los nodos. Puede especificar hasta 64 caracteres para el nombre de nodo. Si especifica más de 64 caracteres, el mandato falla.

nombre_espacio_de_archivos o FSID

Especifica el nombre o el ID de espacio de archivos (FSID) de uno o varios espacios de archivos que se notifican en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. El asterisco es el valor predeterminado. Especifique uno de los siguientes valores:

*

Especifique un asterisco (*) para mostrar todos los espacios de archivos o ID.

nombre_espacio_de_archivos

Especifica el nombre del espacio de archivos. Especifique varios nombres separándolos con comas y sin espacios intercalados. FSID especifica el identificador del espacio de archivos. Este parámetro es válido para los clientes con espacios de archivos que están en formato Unicode. Especifique varios nombres separándolos con comas y sin espacios intercalados.

Para los clientes con espacios de archivos en formato Unicode, puede especificar un nombre de espacio de archivos o un FSID. Si especifica un nombre de espacio de archivos, es posible que el servidor deba convertir el nombre de espacio de archivos que especifique. Por ejemplo, puede que el servidor deba convertir el nombre que especifique de la página de códigos del servidor a Unicode.

Restricciones: Se aplican las siguientes restricciones a los nombres de espacio de archivos y los identificadores de espacio de archivos (FSID):

- Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.
- No especifique FSID y nombres de espacio de archivos en el mismo mandato.

CODEType

Especifica qué tipo de espacios de archivos se van a incluir en el informe. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un asterisco para visualizar información sobre todos los espacios de archivos. Este parámetro es opcional. Especifique uno de los siguientes valores:

UNICODE

Incluir los espacios de archivos que están en formato Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en formato Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos. Este es el valor predeterminado.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro cuando los clientes de IBM Spectrum Protect tengan espacios de archivos en formato Unicode y estén en sistemas operativos Windows, NetWare o Macintosh OS X. Este parámetro es opcional.

Este parámetro es necesario si especifica un nombre de nodo y un nombre de espacio de archivos o un FSID.

Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un asterisco.

Especifique uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del

servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

TODate

Especifica la fecha más reciente de las estadísticas que se van a suprimir. IBM Spectrum Protect elimina únicamente las estadísticas cuya fecha sea la misma o sea anterior a la fecha que especifique. Este parámetro es opcional.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	15/10/2015 Si especifica una fecha, se evaluarán todos los registros candidatos que se grabaron en dicha fecha (que finaliza a las 11:59:59 pm).
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para visualizar la información creada hasta ayer, puede especificar TODATE=TODAY-1 o TODATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los registros que estaban activos el día 10 del mes actual.

TOTime

Especifica que desea suprimir las estadísticas de eliminación de duplicados de datos creadas hasta esa hora inclusive en la fecha indicada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada.	12:30:22
NOW	La hora actual en la fecha especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada.	NOW+03:00 o +03:00. Si emite el mandato DELETE DEDUPSTATS a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect suprime los registros con la hora 12:00 o anterior en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada.	NOW-03:30 o -03:30. Si emite el mandato DELETE DEDUPSTATS a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect suprime los registros con la hora 5:30 o anterior en la fecha especificada.




Ejemplo: suprimir estadísticas de eliminación de duplicados de datos para un espacio de archivos

Suprimir estadísticas de deduplicación de datos de un espacio de archivos llamado /srvr que pertenece a una agrupación de almacenamiento de contenedores de directorio, POOL1, que está almacenada en el nodo de cliente NODE1.

```
delete dedupstats pool1 node1 /srvr
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE DEDUPSTATS

Mandato	Descripción
GENERATE DEDUPSTATS	Genera las estadísticas de eliminación de duplicados de datos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DEDUPSTATS	Muestra las estadísticas de eliminación de duplicados de datos.

DELETE DEVCLASS (Suprimir una clase de dispositivo)

Utilice este mandato para suprimir una clase de dispositivo.

Para utilizar este mandato, antes debe suprimir todas las agrupaciones de almacenamiento asignadas a la clase de dispositivo y, si es necesario, cancelar todos los procesos de exportación o importación de la base de datos que estén utilizando la clase de dispositivo.

No se puede suprimir la clase de dispositivo DISK, que se predefine en la instalación, pero se pueden suprimir todas las clases de dispositivo que haya definido un administrador de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELeTe DEVclass--nombre_clase_dispositivo-----><
```

Parámetros

nombre_clase_dispositivo (Necesario)
Especifica el nombre de la clase de dispositivo que se ha de suprimir.









Ejemplo: suprimir una clase de dispositivo

Suprimir la clase de dispositivo denominada MYTAPE. No existen agrupaciones de almacenamiento asignadas a la clase de dispositivo.

```
delete devclass mytape
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE DEVCLASS

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux UPDATE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Cambia los atributos de una clase de dispositivo para el almacenamiento gestionado por un servidor de medios de z/OS.

DELETE DOMAIN (Suprimir un dominio de políticas)

Utilice este mandato para suprimir un dominio de políticas. Todos los conjuntos de políticas, incluido el conjunto de políticas ACTIVE, clases de gestión y grupos de copia se suprimen junto con el dominio de políticas.

No se puede suprimir un dominio de políticas en el que haya nodos inscritos. Para determinar si hay nodos cliente inscritos para un dominio de políticas, emita el mandato QUERY DOMAIN o QUERY NODE. Traspase todos los nodos cliente a otro dominio de políticas o suprima los nodos.

Puede suprimir el dominio de políticas STANDARD predefinido. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELEte Domain--nombre_dominio-----><
```

Parámetros

nombre_dominio (Necesario)
Especifica el dominio de políticas que se suprime.

Ejemplos: suprimir un dominio de políticas

Suprimir el dominio de políticas EMPLOYEE_RECORDS.

```
delete domain employee_records
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE DOMAIN

Mandato	Descripción
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

DELETE DRIVE (Suprimir una unidad de una biblioteca)

Utilice este mandato para suprimir una unidad de una biblioteca. No se puede suprimir una unidad que se está utilizando.

Todas las rutas relacionadas con una unidad deben suprimirse para que la propia unidad pueda suprimirse.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELEte DRive--nombre_biblioteca--nombre_unidad-----><
```

Parámetros

nombre_biblioteca (Necesario)
Especifica el nombre de la biblioteca donde está situada la unidad.
nombre_unidad (Obligatorio)
Especifica el nombre de la unidad que se ha de suprimir.

Ejemplo: suprimir una unidad de una biblioteca

Suprimir la unidad DRIVE3 de la biblioteca denominada AUTO.

```
delete drive auto drive3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE DRIVE

Mandato	Descripción
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE DRIVE	Cambia los atributos de una unidad.

DELETE EVENT (Suprimir registros de eventos)

Utilice este mandato para suprimir registros de eventos de la base de datos. Se crea un registro de eventos cuando se arranca o falla el proceso de un mandato planificado.

Este mandato suprime únicamente los registros de eventos que existen a la hora que se ejecuta el mandato. Un registro de eventos no se encontrará:

- Si el registro de eventos no se ha creado nunca (el evento se ha planificado para el futuro).
- Si el evento se ha pasado y el registro de eventos ya se ha suprimido.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
                .-00:00-.
>>-DELeTe EVent--fecha--+-----+----->
                '-hora--'

.-TYPE---Client-----
>+-----+-----<
'-TYPE---Client-----'
      +-Administrative+
      '-All-----'
```

Parámetros

fecha (Obligatorio)

Especifica la fecha que se utiliza para determinar qué registros de eventos se han de suprimir. El número máximo de días que puede especificar es de 9999.

Utilice este parámetro junto con el parámetro TIME para especificar una fecha y hora en que suprimir los registros de eventos. Se suprimirá cualquier registro cuyo inicio planificado sea anterior a la fecha y hora especificadas. Sin embargo, no se suprimirán los registros de eventos cuyo margen de puesta en marcha no haya transcurrido todavía.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

hora

Especifica la hora que se utiliza para determinar qué registros de eventos se han de suprimir. Utilice este parámetro junto con el parámetro DATE para especificar una fecha y hora en que suprimir los registros de eventos. Se suprimirá cualquier registro cuyo inicio planificado sea anterior a la fecha y hora especificadas. Sin embargo, no se suprimirán los registros de eventos cuyo margen de puesta en marcha no haya transcurrido todavía. El valor predeterminado es 00:00.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+03:00 o +03:00 Atención: Si emite este mandato a las 9:00 utilizando NOW+03:00 o +03:00, IBM Spectrum Protect suprimirá los registros que tengan una hora a partir de las 12:00 en la fecha que se especifique.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-03:00 o -03:00

TYPE

Especifica el tipo de eventos que se ha de suprimir. Este parámetro es opcional. El valor predeterminado es CLIENT. Los valores posibles son:

Client

Especifica que se suprimen los registros de eventos de las planificaciones de cliente.

ADministrative

Especifica que se suprimen los registros de eventos de las planificaciones de mandatos de administración.

ALL

Especifica que se suprimen los registros de eventos de las planificaciones de mandatos de administración y de cliente.

Ejemplo: suprimir registros de eventos

Suprimir registros para eventos con horas de inicio planificadas anteriores a las 08:00 del 26 de Mayo de 1998 (26/05/1998), y cuyo margen de puesta en marcha ya haya transcurrido. Los registros de estos eventos se suprimirán, con independencia de si ha transcurrido o no el período de retención de los registros de eventos, tal como se ha especificado con el mandato SET EVENTRETENTION.

```
delete event 05/26/1998 08:00
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE EVENT

Mandato	Descripción
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.

DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)

Utilice este mandato para suprimir la definición del servidor de eventos. Debe emitir este mandato antes de emitir el mandato DELETE SERVER. Si especifica el servidor que se ha definido como el servidor de eventos en el mandato DELETE SERVER, recibirá un mensaje de error.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe EVENTSErVer-----<<
```

Ejemplo: suprimir una definición de servidor de eventos

Suprimir la definición del servidor de eventos ASTRO.

```
delete eventserver
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE EVENTSERVER

Mandato	Descripción
DEFINE EVENTSERVER	Define un servidor como un servidor de eventos.
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.

DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)

Utilice este mandato para suprimir espacios de archivos del servidor. Los archivos que pertenecen al espacio de archivos se suprimen de las agrupaciones de almacenamiento primaria, datos activos y de copia, y de los grupos de proximidad de espacio de archivos.

IBM Spectrum Protect suprime uno o varios espacios de archivos como una serie de transacciones de base de datos de proceso por lotes, con lo que impide que se ejecute una operación de retrotracción o validación para todo un espacio de archivos como una sola acción. Si se cancela el proceso o se produce un problema en el sistema, puede realizarse una supresión parcial. Un mandato DELETE FILESPACE posterior para el mismo nodo o propietario puede suprimir los datos restantes.

Si este mandato se aplica a un volumen WORM (una sola grabación, varias lecturas), el volumen se hará reutilizable de nuevo si le queda espacio en el cual se puedan grabar datos. Los datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el mandato CHECKOUT LIBVOLUME.

Consejos:

- Si la protección de retención de archivado está activada, el servidor suprime las copias archivadas con periodos de retención caducados. Para obtener más información, consulte el mandato SET ARCHIVERETENTIONPROTECTION.
- El servidor no suprimirá las copias archivadas que están en espera de supresión hasta que se libere la retención.
- La reclamación no se inicia mientras el mandato DELETE FILESPACE se está ejecutando.
- Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se elimina del grupo de proximidad.
- Si suprime un espacio de archivo en una agrupación de almacenamiento de duplicados eliminados, el nombre del espacio de archivo DELETED aparece en la salida del mandato QUERY OCCUPANCY hasta que se hayan eliminado las dependencias de eliminación de duplicados.
- Cuando se configura la réplica en un espacio de archivos, el mandato DELETE FILESPACE solo suprime el espacio de archivos en el servidor cuando emite el mandato. Si emite el mandato REPLICATE NODE, el espacio de archivos no se suprime en el otro servidor de réplica.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-DElete Filespace--nombre_nodo--nombre_espacio_archivos----->

.-Type----ANY----- .-Data----ANY-----
>-----+-----+-----+-----+-----+----->
'-Type---+-ANY-----+' '-Data---+-ANY-----+'
      +-Backup-----+          +-Files-----+
      +-ARchive-----+          |         (1)   |
      +-SPacemanaged-+          '-IMages-----'
      '-SERver-----'

.-Wait----No-----
>-----+-----+-----+-----+-----+----->
'-Wait---+-No---+' '-OWNer----owner_name-'
      '-Yes-'

.-NAMEType----SERVER-----
>-----+-----+-----+-----+-----+----->
'-NAMEType---+-SERVER---+'
      +-UNICODE-+
      '-FSID----'

.-CODEType----BOTH-----
>-----+-----+-----+-----+-----+-----><
'-CODEType---+-UNICODE---+'
      +-NONUNICODE-+
      '-BOTH-----'
```

Notas:

1. Este parámetro solo se puede utilizar cuando se especifica `TYPE=ANY` o `TYPE=BACKUP`.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente al que pertenece el espacio de archivos.

nombre_espacio_archivos (Necesario)

Especifica el nombre del espacio de archivos que se ha de suprimir. Este nombre es sensible a las mayúsculas y minúsculas y debe entrarse exactamente tal y como lo conoce el servidor. Para determinar cómo ha de especificarse el nombre, utilice el mandato `QUERY FILESPACE`. Puede utilizar caracteres comodín para especificar este nombre.

Para un servidor que tenga clientes que admiten Unicode, es posible que deba utilizar el servidor para que éste convierta el nombre del espacio de archivos que especifica. Por ejemplo, es posible que desee que el servidor convierta el nombre especificado de la página de códigos del servidor a Unicode. Consulte el parámetro `NAMETYPE` para obtener información detallada. Si no especifica ningún nombre de espacio de archivos o especifica sólo un único carácter comodín para el nombre, puede utilizar el parámetro `CODETYPE` para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

Type

Especifica el tipo de datos que se ha de suprimir. Este parámetro es opcional. El valor predeterminado es `ANY`. Pueden usarse los valores siguientes:

ANY

Sólo se suprimen las versiones de copia de seguridad de los archivos y las copias archivadas.

Si especifica `delete filespace nombre_nodo * type=any`, se suprimirán todos los datos de copias archivadas y de copias de seguridad de todos los espacios de archivos para ese nodo. Los espacios de archivos solo se suprimen si no contienen archivos movidos desde un cliente de IBM Spectrum Protect for Space Management.

Backup

Se suprimen los datos de copia de seguridad del espacio de archivos.

ARchive

Se suprimen todos los datos archivados en el servidor para el espacio de archivos.

SPacemanaged

Se suprimen los archivos migrados desde el sistema de archivos local de un usuario mediante un cliente de IBM Spectrum Protect for Space Management. Se ignora el parámetro OWNER cuando especifica TYPE=SPACEMANAGED.

SERver

Se suprimen todas las copias archivadas de todos los espacios de archivos de un nodo inscrito como TYPE=SERVER.

DAta

Especifica los objetos a suprimir. Este parámetro es opcional. El valor predeterminado es ANY. Puede especificar uno de los siguientes valores:

ANY

Se suprimen archivos, directorios e imágenes.

FIles

Se suprimen archivos y directorios.

IMages

Se suprimen objetos de imágenes. Puede utilizar este parámetro solamente si ha especificado TYPE=ANY o TYPE=BACKUP.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los siguientes valores:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Yes

Especifica que el servidor procesa este mandato en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida al cliente de administración cuando finaliza el mandato.
Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

OWNer

Restringe los datos que se suprimen a los archivos que pertenecen al propietario. Este parámetro es opcional y se hace caso omiso cuando TYPE=SPACEMANAGED. Este parámetro sólo se aplica a los sistemas cliente de varios usuarios, como AIX, Linux y Solaris OS.

NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Un cliente de archivado y copia de seguridad con soporte Unicode solamente está disponible para los siguientes sistemas operativos: Windows, Macintosh OS X y NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNIcode

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

CODEType

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

UNIcode

Incluir los espacios de archivos que están en Unicode.

NONUNIcode

Incluir los espacios de archivos que no están en Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

Suprimir un espacio de archivos

Suprime el espacio de archivo C_Drive que pertenece al nodo cliente HTANG.

```
delete filespace htang C_Drive
```

Suprimir todos los archivos gestionados por espacio para un nodo de cliente

Suprimir todos los archivos migrados del nodo de cliente APOLLO (esto es, todos los archivos gestionados por espacio).

```
delete filespace apollo * type=spacemanaged
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE FILESPACE

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
RENAME FILESPACE	Redenomina un espacio de archivos de cliente en el servidor.

DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)

Utilice este mandato para suprimir de un grupo de servidores un servidor o un grupo de servidores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
      .,-----  
      v |  
>>-DELeTe GRPMEMber--nombre_grupo----nombre_miembro-+-----><
```

Parámetros

nombre_grupo (Obligatorio)

Especifica el grupo.

nombre_miembro (Obligatorio)

Especifica el servidor o el grupo que se suprime del grupo. Para especificar varios nombres, debe separarlos con comas y sin espacios intercalados.

Ejemplo: suprimir un servidor de un grupo de servidores

Suprimir el miembro PHOENIX del grupo WEST_COMPLEX.

```
delete grpmember west_complex phoenix
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE GRPMEMBER

Mandato	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVER	Suprime la definición de un servidor.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

DELETE LIBRARY (Suprimir una biblioteca)

Utilice este mandato para suprimir una biblioteca. Antes de suprimir la biblioteca, deberá eliminar otros objetos asociados, por ejemplo la ruta.

Utilice este mandato para suprimir una biblioteca. Antes de suprimir una biblioteca, suprima la ruta y todas las unidades asociadas.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELeTe LIBRary--nombre_biblioteca----->>
```

Parámetros

nombre_biblioteca (Necesario)
Especifica el nombre de la biblioteca que se ha de suprimir.

Ejemplo: suprimir una biblioteca manual

Suprimir la biblioteca manual denominada LIBR1.

```
delete library libr1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE LIBRARY

Mandato	Descripción
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.

Mandato	Descripción
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE PATH	Cambia los atributos asociados con una ruta.

DELETE MACHINE (Suprimir información de una máquina)

Utilice este mandato para suprimir la información de descripción de una máquina. Para sustituir la información existente, emita este mandato y, a continuación, emita el mandato INSERT MACHINE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe MACHine--machine_name----->
. -Type---All-----
>+-----+----->
' -Type---All-----+'
      +-RECOVERYInstructions-+
      '-Characteristics-----'
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina cuya información debe suprimirse.

Type

Especifica el tipo de información de la máquina. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

All

Especifica toda la información.

RECOVERYInstructions

Especifica las instrucciones de recuperación.

CHaracteristics

Especifica las características de la máquina.

Ejemplo: suprimir la información de una máquina específica

Suprimir las características de máquina asociadas a la máquina DISTRICT5.

```
delete machine district5 type=characteristics
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE MACHINE

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE MACHINE	Cambia la información para una máquina.

DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)

Utilice este mandato para suprimir la asociación que hay entre una máquina y uno o varios nodos. Este mandato no suprime el nodo de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELEte MACHNODEAssociation--machine_name----nombre_nodo+----><
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de una máquina que está asociada a uno o varios nodos.

nombre_nodo (Obligatorio)

Especifica el nombre de un nodo asociado a una máquina. Si especifica una lista de nombres de nodos, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Si un nodo no está asociado a la máquina, se omite ese nodo.

Ejemplo: suprimir una asociación entre un nodo y una máquina

Suprimir la asociación entre la máquina DISTRICT5 y el nodo ACCOUNTSPAYABLE.

```
delete machnodeassociation district5 accountspayable
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE MACHNODEASSOCIATION

Mandato	Descripción
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
QUERY MACHINE	Muestra información sobre máquinas.

DELETE MGMTCLASS (Suprimir una clase de gestión)

Utilice este mandato para suprimir una clase de gestión. No puede suprimir una clase de gestión del juego de políticas ACTIVE. Junto con la clase de gestión, se suprimen todos los grupos de copia de la clase de gestión.

Puede suprimir la clase de gestión asignada como valor predeterminado para un juego de políticas, pero un juego de políticas no se puede activar si no tiene una clase de gestión predeterminada.

Puede suprimir la clase de gestión predefinida STANDARD del dominio de políticas STANDARD. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la clase de gestión.

Sintaxis

```
>>-DELEte MGmtclass--nom_dominio--nom_conjunto_políticas--nom_clase-><
```


Parámetros

- nombre_dominio (Necesario)
Especifica el dominio de políticas al que pertenece la clase de gestión.
- nombre_juego_políticas (Necesario)
Especifica el juego de políticas al que pertenece la clase de gestión.
- nom_clase (Necesario)
Especifica la clase de gestión que se suprime.

Ejemplo: suprimir una clase de gestión

Suprimir la clase gestión ACTIVEFILES del juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS.

```
delete mgmtclass employee_records  
vacation activefiles
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE MGMTCLASS

Mandato	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

DELETE NODEGROUP (Suprimir un grupo de nodos)

Utilice este mandato para suprimir un grupo de nodos. No puede suprimir un grupo de nodos si incluye algún miembro.

Atención: Puede eliminar todos los miembros del grupo de nodos ejecutando el mandato DELETE NODEGROUPMEMBER con un carácter comodín en el parámetro nombre_nodo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-DELeTe NODEGroup--nombre_grupo-----<<
```

Parámetros

- nombre_grupo
Especifica el nombre del grupo de nodos que desea suprimir.

Ejemplo: suprimir un grupo de nodos

Suprimir un grupo de nodos denominado group1.

```
delete nodegroup group1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE NODEGROUP

Mandato	Descripción
---------	-------------

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)

Utilice este mandato para suprimir un nodo cliente de un grupo de nodos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```

      .-.-.-.-.-.
      v         |
>>-DELEte NODEGROUPMember--nombre_grupo----nombre_nodo-+-----><

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de nodos del que desea suprimir un nodo cliente.

nombre_nodo

Especifica el nombre del nodo cliente que desea suprimir del grupo de nodos. Puede especificar uno o más nombres. Al especificar varios nombres, separe los nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nodos.

Ejemplo: suprimir miembros de grupo de nodos

Suprimir dos nodos, `node1` y `node2`, de un grupo de nodos, `group1`.

```
delete nodegroupmember group1 node1,node2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE NODEGROUPMEMBER

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.

Mandato	Descripción
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

DELETE PATH (Suprimir una ruta)

Utilice este mandato para suprimir una definición de ruta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELeTe PATH--nombre_origen--nombre_destino----->
                                     (1)
>--SRCType-----+--DATAMover-----+----->
      '-SERVer-----'
                                     (2)
>--DESTType-----+--DRive-----LIBRary-----nombre_biblioteca+----<
      '-LIBRary-----'
```

Notas:

1. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.
2. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.

Parámetros

nombre_origen (Obligatorio)

Especifica el origen de la ruta que se va a suprimir. Este parámetro es necesario.

El nombre especificado debe ser el nombre de un servidor o transportador de datos que ya se haya definido para el servidor.

nombre_destino (Obligatorio)

Especifica el nombre del destino de la ruta que se va a suprimir. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen de la ruta que se va a suprimir. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

DESTType (Obligatorio)

Especifica el tipo de destino. Los valores posibles son:

DRive LIBRary=library_name

Especifica que el destino es una unidad. Los parámetros DRIVE y LIBRARY son necesarios si el tipo de destino es una unidad.

LIBRary

Especifica que el destino es una biblioteca.

Atención: Si se suprime la ruta de un transportador de datos a una biblioteca, o se suprime la ruta del servidor a una biblioteca, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia en este estado, no se inicializará la biblioteca.

Ejemplo: suprimir una ruta de transportador de datos NAS

Suprimir una ruta de un transportador de datos NAS denominado NAS1 a la biblioteca NASLIB.

```
delete path nas1 naslib srctype=datamover desttype=library
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE PATH

Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE PATH	Define una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE PATH	Cambia los atributos asociados con una ruta.

DELETE POLICYSET (Suprimir un juego de políticas)

Utilice este mandato para suprimir un juego de políticas. Al suprimir un juego de políticas, también se suprimen todas las clases de gestión y los grupos de copia que pertenecen al juego de políticas.

El conjunto de políticas ACTIVE de un dominio de políticas no se puede suprimir. Puede sustituir el contenido del conjunto de políticas ACTIVE activando otro conjunto de políticas. De lo contrario, el único modo de eliminar el conjunto de políticas ACTIVE es suprimir el dominio de políticas que contiene el conjunto de políticas.

Puede suprimir el juego de políticas STANDARD predefinido. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-DELeTe Policyset--nombre_dominio--nombre_juego_políticas----><
```

Parámetros

nombre_dominio (Necesario)
Especifica el dominio de políticas al que pertenece el juego de políticas.

nombre_juego_políticas (Necesario)
Especifica el juego de políticas que se va a suprimir.

Ejemplo: suprimir un juego de políticas

Suprima el conjunto de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS emitiendo el mandato siguiente:

```
delete policyset employee_records vacation
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.

Parámetros

nombre_perfil (Obligatorio)

Especifica el perfil donde se suprimen las asociaciones.

ADMins

Especifica los administradores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (*) para suprimir del perfil todos los administradores. Si especifica una lista de administradores y para el perfil existe una definición que coincide con todos, el mandato no se ejecutará. Las definiciones de administrador no se modifican en el gestor de configuración. Sin embargo, se suprimen automáticamente de todos los servidores gestionados suscritos en la siguiente renovación de la configuración, con las excepciones siguientes:

- Un administrador no se suprime si tiene una sesión abierta en el servidor.
- Un administrador no se suprime si, como consecuencia, el servidor gestionado se queda sin administradores con la clase de privilegio de sistema.

DOmains

Especifica los dominios cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (*) para suprimir del perfil todos los dominios. Si especifica una lista de dominios y para el perfil existe una definición que coincide con todos los dominios, el mandato no se ejecutará.

La información de dominio se suprime automáticamente de todos los servidores gestionados suscritos. Sin embargo, no se suprimirá un dominio de políticas que tenga nodos cliente asignados. Para suprimir el dominio en el servidor gestionado, asigne esos nodos cliente a otro dominio de políticas.

ADSCHeds

Especifica una lista de planificaciones de administración cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Si especifica una lista de planificaciones de administración y para el perfil existe una definición que coincide con todas las planificaciones de administración, el mandato no se ejecutará. Utilice el carácter de coincidencia con todos (*) para suprimir del perfil todas las planificaciones de administración.

Las planificaciones de administración se suprimen automáticamente de todos los servidores gestionados suscritos. Sin embargo, una planificación de administración no se suprime si está activa en el servidor gestionado. Para suprimir una planificación activa, debe convertir la planificación en inactiva.

SCRipts

Especifica los scripts de mandatos del servidor cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (*) para suprimir del perfil todos los scripts. Si especifica una lista de dominios y para el perfil existe una definición que coincide con todos los scripts, el mandato no se ejecutará. Los scripts de mandatos del servidor se suprimen automáticamente de todos los servidores gestionados suscritos.

CLOptsets

Especifica los conjuntos de opciones de cliente cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (*) para suprimir del perfil todos los conjuntos de opciones de cliente. Si especifica una lista de conjuntos de opciones de cliente y para el perfil existe una definición que coincide con todos los conjuntos de opciones de cliente, el mandato no se ejecutará. Los conjuntos de opciones de cliente se suprimen automáticamente de todos los servidores gestionados suscritos.

SERVers

Especifica los servidores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Puede utilizar el carácter de coincidencia con todos (*) para suprimir del perfil todos los servidores. Si especifica una lista de servidores y para el perfil existe una definición que coincide con todos los servidores, el mandato no se ejecutará. Las definiciones de servidor se suprimen automáticamente de todos los servidores gestionados suscritos con las excepciones siguientes:

- Una definición de servidor no se suprime si el servidor gestionado tiene una conexión abierta con otro servidor.
- Una definición de servidor no se suprime si el servidor gestionado tiene una clase de dispositivo de tipo SERVER que hace referencia al otro servidor.
- Una definición de servidor no se suprime si el servidor es el servidor de eventos para el servidor gestionado.

SERVERGroups

Especifica los grupos de servidores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Puede utilizar el carácter de coincidencia con todos (*) para suprimir del perfil todos los grupos de servidores. Si especifica una lista de grupos de servidores y para el perfil existe una definición que coincide con todos los grupos, el mandato no se ejecutará. Las definiciones de grupo de servidores se suprimen automáticamente de todos los servidores gestionados suscritos.

Ejemplo: suprimir las asociaciones de dominio de un perfil específico

Suprimir todas las asociaciones de dominios del perfil denominado MIKE.

```
delete profassociation mike domains=*
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE PROFASSOCIATION

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

DELETE PROFILE (Suprimir un perfil)

Utilice este mandato en un gestor de configuración para suprimir un perfil y detener su distribución a los servidores gestionados.

No se puede suprimir un perfil bloqueado. Primero debe desbloquear el perfil con el mandato UNLOCK PROFILE.

Al suprimir un perfil de un gestor de configuración no se suprimen de los servidores gestionados los objetos asociados con ese perfil. Puede utilizar el mandato DELETE SUBSCRIPTION con el parámetro DISCARDOBJECTS=YES en cada servidor gestionado suscrito para suprimir suscripciones al perfil y objetos asociados. De este modo también se evita que los servidores gestionados soliciten actualizaciones adicionales del perfil.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe PROFIle--nombre_perfil--+-Force---No-----+-----><
                                     '-Force---No---+'
                                     '-Yes-'
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el perfil que se suprime.

Force

Especifica si se suprime el perfil en caso de que uno o más servidores gestionados estén suscritos a dicho perfil. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que no se suprime el perfil si uno o más servidores gestionados están suscritos a dicho perfil. Se pueden suprimir las suscripciones en cada servidor gestionado con el mandato DELETE SUBSCRIPTION.

Yes

Especifica que se suprime el perfil aunque uno o más servidores gestionados estén suscritos a dicho perfil. Cada servidor inscrito continúa solicitando actualizaciones del perfil suprimido hasta que se suprima la inscripción.

Ejemplo: suprimir un perfil

Suprimir un perfil denominado BETA, aunque se inscriban en él uno o varios servidores gestionados.

```
delete profile beta force=yes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)

Utilice este mandato para suprimir la asociación de una o varias máquinas a un medio de recuperación. Este mandato no suprime la máquina de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe RECMEDMACHAssociation--nombre_medio----->
      .-,-----
      v          |
>----nombre_máquina-+-----<<
```

Parámetros

nombre_soporte (Obligatorio)

Especifica el nombre del medio de recuperación que está asociado a una o varias máquinas.

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina asociada al medio de recuperación. Para especificar una lista de nombres de máquinas, debe separar los nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Si una máquina no está asociada al medio de recuperación, la máquina no se tiene en cuenta.

Ejemplo: suprimir la asociación de una máquina a los medios de recuperación

Suprimir la asociación entre el medio de recuperación DIST5RM y las máquinas DISTRICT1 y DISTRICT5.

```
delete recmedmachassociation  
dist5rm district1,district5
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE RECMEDMACHASSOCIATION

Mandato	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
QUERY MACHINE	Muestra información sobre máquinas.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

DELETE RECOVERYMEDIA (Suprimir medio de recuperación)

Utilice este mandato para suprimir una definición de medio de recuperación de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe RECOVeRYMedia--nombre_medio----->>
```

Parámetros

nombre_soporte (Obligatorio)
Especifica el nombre del medio de recuperación.

Ejemplo: suprimir la definición de los medios de recuperación

Suprimir el medio de recuperación DIST5RM.

```
delete recoverymedia dist5rm
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE RECOVERYMEDIA

Mandato	Descripción
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

DELETE SCHEDULE (Suprimir una planificación de cliente o de mandato de administración)

Utilice este mandato para suprimir planificaciones de la base de datos.

El mandato DELETE SCHEDULE tiene dos formatos: uno si la planificación se aplica a las operaciones de cliente y el otro si la planificación se aplica a mandatos administrativos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con DELETE SCHEDULE

Mandato	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
QUERY SCHEDULE	Muestra información sobre planificaciones.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- DELETE SCHEDULE (Suprimir una planificación de cliente)
Utilice el mandato DELETE SCHEDULE para suprimir de la base de datos una o varias planificaciones de cliente. Cuando se elimina la planificación, se suprimen todas las asociaciones de cliente con dicha planificación.
- DELETE SCHEDULE (Suprimir una planificación de administración)
Utilice este mandato para suprimir de la base de datos una o varias planificaciones de mandato de administración.

DELETE SCHEDULE (Suprimir una planificación de cliente)

Utilice el mandato DELETE SCHEDULE para suprimir de la base de datos una o varias planificaciones de cliente. Cuando se elimina la planificación, se suprimen todas las asociaciones de cliente con dicha planificación.

Clase de privilegio

Para suprimir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado para el dominio de políticas al que pertenece la planificación.

Sintaxis

```
>>-DElete SChedule--nombre_dominio--nombre_planificación----->
      .-Type-----Client-.
>--+-----+-----><
```

Parámetros

- nombre_dominio (Necesario)
Especifica el nombre del dominio de políticas al que pertenece la planificación.
- nombre_planificación (Obligatorio)
Especifica el nombre de la planificación que se va a suprimir. Puede utilizar un carácter comodín para especificar este nombre.
- Type=Client
Especifica que se suprimirá una planificación de cliente. Este parámetro es opcional. El valor predeterminado es CLIENT.

Ejemplo: suprimir una planificación específica de un dominio de políticas específico

Suprimir la planificación WEEKLY_BACKUP, la cual pertenece al dominio de políticas EMPLOYEE_RECORDS.

```
delete schedule employee_records weekly_backup
```

DELETE SCHEDULE (Suprimir una planificación de administración)

Utilice este mandato para suprimir de la base de datos una o varias planificaciones de mandato de administración.

Clase de privilegio

Para suprimir una planificación de mandatos de administración, debe tener autorización del sistema.

Sintaxis

```
>>-DElete SChedule--schedule_name--Type-----Administrative-----><
```

Parámetros

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación que se va a suprimir. Puede utilizar un carácter comodín para especificar este nombre.

Type=Administrative (Necesario)

Especifica que se suprimirá una planificación de mandato de administración.

Ejemplo: suprimir una planificación de mandatos de administración

Suprimir la planificación de mandato de administración denominada DATA_ENG.

```
delete schedule data_eng type=administrative
```

DELETE SCRATCHPADENTRY (Suprimir una entrada de registro)

Utilice este mandato para suprimir una o varias líneas de datos de un área de registro.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELEte SCRATCHPadentry--major_category--minor_category----->
      .-Line-----*-----
>--subject--+-----+-----><
      '-Line ---número-'
```

Parámetros

major_category (obligatorio)

Especifica la categoría de la que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

minor_category (obligatorio)

Especifica la categoría secundaria de la que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)

Especifica el asunto del que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

Line

Especifica una línea de datos que se suprimirá. Para número, entre el número de la línea que se suprimirá. Todos los datos en la línea se suprimirán. La numeración de otras líneas en la sección de asunto no se ve afectada. Puede suprimir todas las líneas de datos de una sección de asunto omitiendo el parámetro Line en este mandato.

Ejemplo: Suprima todas las líneas de datos de un asunto en el registro

Suprima todas las líneas de datos acerca de la ubicación de un administrador, Jane, de la base de datos que almacena información sobre administradores:

```
delete scratchpadentry admin_info location jane
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SCRATCHPADENTRY

Mandato	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.

Mandato	Descripción
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

DELETE SCRIPT (Suprimir líneas de mandatos de un script o suprimir todo el script)

Utilice este mandato para suprimir una única línea de un script de IBM Spectrum Protect o para suprimir el script de IBM Spectrum Protect completo.

Clase de privilegio

Para emitir este mandato, el administrador debe haber definido el script con anterioridad o debe tener privilegio de sistema.

Sintaxis

```
>>-DELEte SCRipt--nombre_script--+-----+----->>
                        '-Line ----número-'
```

Parámetros

nombre_script (Obligatorio)

Especifica el nombre del script que se va a suprimir. Se suprime el script si no se especifica un número de línea.

Line

Especifica el número de la línea que se va a suprimir del script. Si no especifica ningún número de línea, se suprime todo el script.

Ejemplo: suprimir una línea específica de un script

Mediante la utilización del siguiente script, denominado QSAMPLE, emitir un mandato para suprimir de éste la línea 005.

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY PROCESS

delete script qsampl line=5
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SCRIPT

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

DELETE SERVER (Suprimir una definición de servidor)

Utilice este mandato para suprimir una definición de servidor.

El mandato no se ejecutará si el servidor:

- Está definido como el servidor de eventos.
- Está especificado en una definición de clase de dispositivo cuyo tipo de dispositivo es SERVER.
- Tiene una conexión abierta con otro servidor.
- Es un servidor de destino para los volúmenes virtuales.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe--SERVer--nombre_servidor-----><
```

Parámetros

nombre_servidor (Obligatorio)
Especifica el nombre de un servidor.

Ejemplo: suprimir la definición de un servidor

Suprimir la definición del servidor denominado SERVER2.

```
delete server server2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SERVER

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
UPDATE SERVER	Actualiza la información sobre un servidor.

DELETE SERVERGROUP (Suprimir un grupo de servidores)

Utilice este mandato para suprimir un grupo de servidores. Si el grupo que se suprime es miembro de otros grupos de servidores, IBM Spectrum Protect también elimina el grupo de los otros grupos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe SERVERGroup--nombre_grupo-----><
```

Parámetros

nombre_grupo (Obligatorio)
Especifica el grupo de servidores que se suprime.

Ejemplo: suprimir un grupo de servidores

Suprimir un grupo de servidores denominado WEST_COMPLEX.

```
delete servergroup west_complex
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SERVERGROUP

Mandato	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)

Utilice este mandato para suprimir la definición del desencadenante de espacio de agrupación de almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-DELeTe SPACETriGger--STG----->
>--+-----+----->
  '-STGPOOL----nombre_agrupación_almacenamiento-'
```

Parámetros

STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

STGPOOL

Especifica el desencadenante de la agrupación de almacenamiento que se suprimirá. Si se especifica STG sin especificar STGPOOL, el desencadenante de espacio de la agrupación de almacenamiento predeterminado es el destino de supresión.

Ejemplo: suprimir una definición de desencadenante de espacio

Suprimir la definición del desencadenante de espacio para la agrupación de almacenamiento WINPOOL1.

```
delete spacetrigger stg stgpool=winpool1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SPACETRIGGER

Mandato	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)

Utilice este mandato para suprimir un umbral de supervisión de estado existente.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe STATusthreshold--nombre_umbral-----<<
```

Parámetros

nombre_umbral (Necesario)
Especifica el nombre de umbral que desea suprimir.

Suprimir un umbral de estado existente

Suprima un umbral de estado existente emitiendo el mandato siguiente:

```
delete statusthreshold avgstgpl
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE STATUSTHRESHOLD

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

DELETE STGPOOL (Suprimir una agrupación de almacenamiento)

Utilice este mandato para suprimir una agrupación de almacenamiento. Para suprimir una agrupación de almacenamiento, antes debe suprimir todos los volúmenes que están asignados a la agrupación de almacenamiento.

No se puede suprimir una agrupación de almacenamiento que se identifica como la próxima agrupación de almacenamiento para otra agrupación de almacenamiento. Para obtener más información acerca de la jerarquía de las agrupaciones de almacenamiento, consulte el parámetro NEXTSTGPOOL en el mandato DEFINE STGPOOL.

Restricciones:

- Para las agrupaciones de almacenamiento de contenedor, suprima todos los directorios de agrupación de almacenamiento antes de suprimir la agrupación de almacenamiento.
- No suprima una agrupación de almacenamiento que se especifique como un destino de clase de gestión o grupo de copia del juego de políticas ACTIVE. Es posible que como consecuencia no puedan ejecutarse las operaciones de cliente.
- Cuando suprime una agrupación de almacenamiento de copia que anteriormente se había incluido en una definición de agrupación de almacenamiento primaria (específicamente en la lista COPYSTGPOOLS), debe eliminar la agrupación de almacenamiento de copia de la lista antes de suprimirla. De otro modo, el mandato DELETE STGPOOL no se ejecutará correctamente hasta que se hayan eliminado todas las referencias a esa agrupación de copia. Para cada agrupación de almacenamiento primaria que tenga una referencia a la agrupación de almacenamiento de copia que va a suprimirse, elimine la referencia, mediante la especificación del mandato UPDATE STGPOOL con el parámetro COPYSTGPOOLS, que se hace a todas las agrupaciones de almacenamiento de copia anteriores, a excepción de la agrupación de almacenamiento de copia que va a suprimirse.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe STGpool--nombre_agrupación-----<<
```

Parámetros

nombre_agrupación (Obligatorio)
Especifica la agrupación de almacenamiento que se suprime.





Ejemplo: suprimir una agrupación de almacenamiento

Suprimir la agrupación de almacenamiento denominada POOLA.

```
delete stgpool poola
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE STGPOOL

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
 Sistemas operativos AIX  Sistemas operativos Windows SET DRMCOPYSTGPOOL	 Sistemas operativos AIX  Sistemas operativos Windows Especifica que DRM gestiona las agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

Utilice este mandato para suprimir una definición de un directorio de agrupación de almacenamiento.

Es posible que desee suprimir un directorio de agrupación de almacenamiento por las siguientes razones:

- Para poner fuera de servicio un almacenamiento anterior.
- Para dejar de utilizar el disco local antes de mover datos a la nube.
- Para no mantener los datos en el directorio de agrupación de almacenamiento porque no hay necesidad de hacerlo.

Restricciones:

- Sólo puede emitir este mandato cuando no haya ningún contenedor asignado al directorio de agrupación de almacenamiento. Emita el mandato QUERY CONTAINER para determinar si hay algún contenedor asignado al directorio de agrupación de almacenamiento.
- Para eliminar contenedores de un directorio de agrupación de almacenamiento, debe emitir el mandato UPDATE STGPOOLDIRECTORY y especificar el parámetro ACCESS=DESTROYED. A continuación, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED. Verifique que la máquina se ha eliminado. El parámetro ACTION=REMOVEDAMAGED elimina la información de inventario de los objetos de los que se ha efectuado una copia de seguridad o que han sido archivados. Solo debe eliminar la información de inventario si no necesita las copias de seguridad.

Si el hardware genera algún error o una pérdida del directorio, consulte los mandatos relevantes AUDIT y REPAIR. Debería realizar las reparaciones necesarias en el entorno de IBM Spectrum Protect antes de suprimir la agrupación de almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DElete STGPOOLDIrectory--nombre_agrupación--directorio-----><
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que contiene el directorio que se debe suprimir. Este parámetro es necesario.

directorio (Obligatorio)

Especifica el directorio del sistema de archivos de la agrupación de almacenamiento que se debe suprimir. Este parámetro es necesario.

Ejemplo: actualizar un directorio de agrupación de almacenamiento para preparar la supresión

Actualice un directorio de agrupación de almacenamiento que se denomina DIR1 en la agrupación de almacenamiento POOLA para marcarlo como destruido. Cuando una agrupación de almacenamiento se marca como destruida, puede suprimirla.

 Sistemas operativos AIX  Sistemas operativos Linux

```
update stgpooldirectory poola /storage/dir1 access=destroyed
```

 Sistemas operativos Windows


```
update stgpooldirectory poola e:\storage\dir1 access=destroyed
```

Ejemplo: suprimir un directorio de agrupación de almacenamiento

Suprima el directorio de agrupación de almacenamiento denominado DIR1 en la agrupación de almacenamiento POOLA.

 Sistemas operativos AIX  Sistemas operativos Linux

```
delete stgpooldirectory poola /storage/dir1
```

 Sistemas operativos Windows

```
delete stgpooldirectory poola e:\storage\dir1
```

Tabla 1. Mandatos relacionados con DELETE STGPOOLDIRECTORY

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.
QUERY EXTENTUPDATES	Muestra información sobre las actualizaciones de las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio.

DELETE STGRULE (Suprimir reglas de almacenamiento para agrupaciones de almacenamiento)

Utilice este mandato para suprimir reglas de almacenamiento para una o más agrupaciones de almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe STGRULE--nombre_regla-----<<
```

Parámetros

nombre_regla(Necesario)

Especifica el nombre de la regla de almacenamiento que debe suprimirse. La longitud máxima del nombre es de 30 caracteres.

Suprimir una regla de almacenamiento

Suprimir una regla de almacenamiento llamada stgrule1:

```
delete stgrule stgrule1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE STGRULE

Mandato	Descripción
DEFINE STGRULE	Define una regla de almacenamiento para las agrupaciones de almacenamiento.
QUERY STGRULE	Visualizar información sobre reglas de almacenamiento.
UPDATE STGRULE	Actualiza una regla de almacenamiento para las agrupaciones de almacenamiento.

DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)

Utilice este mandato en un gestor de configuración para suprimir de la base de datos del gestor de configuración suscripciones del servidor gestionado. Utilice este mandato cuando ya no exista un servidor gestionado o no pueda enviar notificaciones al gestor de configuración después de suprimir una suscripción.

Atención: Utilice este mandato sólo en las escasas situaciones en las que la base de datos del gestor de configuración contenga una entrada para una suscripción, pero el servidor gestionado no tenga dicha suscripción. Por ejemplo, utilice este mandato si ya no existe un servidor gestionado o no puede enviar notificaciones al gestor de configuración tras suprimir una suscripción.

En circunstancias normales, utilice el mandato DELETE SUBSCRIPTION para suprimir una suscripción del servidor gestionado. El servidor gestionado envía la notificación al gestor de configuración, que entonces suprime la suscripción de su base de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe SUBSCRIBer--nombre_servidor-----><
```

Parámetros

nombre_servidor (Obligatorio)

Especifica el nombre del servidor gestionado con entradas de suscripción que se deben suprimir.

Ejemplo: suprimir entradas de suscripción para un servidor gestionado específico

Suprimir todas las entradas de suscripción para un servidor gestionado denominado DAN.

```
delete subscriber dan
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SUBSCRIBER

Mandato	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)

Utilice este mandato en un servidor gestionado para suprimir una suscripción a un perfil. También puede suprimir del servidor gestionado todos los objetos asociados al perfil.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe SUBSCRIPtion--nombre_perfil----->  
.-DISCARDobjects----No-----.  
>>+-----+-----><  
'-DISCARDobjects----++-No---'
```

'-Yes-'

Parámetros

nombre_perfil (Obligatorio)

Especifica el nombre del perfil cuya inscripción se suprime.

DISCARDobjects

Especifica si los objetos asociados con el perfil se van a suprimir en el servidor gestionado. Este parámetro es opcional. El valor predeterminado es NO.

No

Especifica que los objetos no se suprimirán.

Yes

Especifica que se suprimirán los objetos, excepto si están asociados a otro perfil para el que hay una inscripción definida.

Ejemplo: suprimir una suscripción de perfil

Suprimir una suscripción a un perfil denominado ALPHA y sus objetos asociados de un servidor gestionado.

```
delete subscription alpha discardobjects=yes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE SUBSCRIPTION

Mandato	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)

Utilice este mandato para suprimir una definición de correlación de espacios de archivos virtuales. Los espacios de archivos virtuales que contienen datos no puede suprimirse a menos que primero se utilice el mandato DELETE FILESPACE.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

Sintaxis

```
>>-DElete VIRTUALFSmapping -nombre_nodo----->  
>---nombre_espacio_archivos_virtual-----><
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre_espacio_archivos_virtual (Obligatorio)

Especifica el nombre de la definición de correlación de espacios de archivos virtuales que se suprimirá. Se permite el uso de caracteres comodín.

Ejemplo: suprimir una correlación de espacios de archivos virtuales

Suprimir la definición de correlación de espacios de archivos virtuales /mikeshomedir para el nodo NAS denominado NAS1.

```
delete virtualfsmapping nas1 /mikeshomedir
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE VIRTUALFSMAPPING

Mandato	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

DELETE VOLHISTORY (Suprimir información histórica de volúmenes)

Utilice este mandato para suprimir los registros del archivo histórico de volúmenes que ya no son necesarios (por ejemplo, los registros de volúmenes de copia de seguridad de la base de datos obsoletos).

Cuando suprime registros de volúmenes que no se encuentran en las agrupaciones de almacenamiento (por ejemplo, volúmenes de copia de seguridad de la base de datos o de exportación), los volúmenes volverán al estado reutilizable aunque IBM Spectrum Protect los haya adquirido como volúmenes privados. Se suprimirán los volúmenes reutilizables con el tipo de dispositivo FILE. Al suprimir los registros de volúmenes de agrupación de almacenamiento, los volúmenes permanecen en la base de datos de IBM Spectrum Protect. Al suprimir registros de objetos de archivo del plan de recuperación de un servidor origen, los objetos del servidor destino se marcan para suprimirlos.

Restricción: No utilice el mandato DELETE VOLHISTORY para suprimir del archivo histórico de volúmenes la información sobre volúmenes correspondiente al conjunto de copias de seguridad. En su lugar, utilice el mandato DELETE BACKUPSET para ello.

Los usuarios de DRM, deben controlar la caducidad de la copia de seguridad de base de datos con el mandato SET DRMDBBACKUPEXPIREDAYS y no con este mandato DELETE VOLHISTORY. Utilice el mandato DELETE VOLHISTORY para eliminar un registro del volumen. Esto puede provocar la pérdida de los volúmenes gestionados con el mandato MOVE DRMEDIA. Utilice el mandato SET DRMDBBACKUPEXPIREDAYS para gestionar la caducidad automática de los volúmenes de copia de seguridad de base de datos DRM.

Consejos:

- No se suprimen los volúmenes de la serie de copia de seguridad de la base de datos más reciente.
- Los archivos históricos de volúmenes existentes no se actualizan automáticamente con este mandato.
- Puede utilizar el mandato DEFINE SCHEDULE para suprimir registros del archivo histórico de forma periódica.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DELeTe VOLHistory--TODate-----fecha----->
      .-TOTime-----23:59:59-.
>>+-----+----->
      '-TOTime-----hora-----'

>>-Type-----+All-----<
      +-DBBackup--+-----+
      |           '-DEVclass---class_name-' |
      +-DBSnapshot--+-----+
      |           '-DEVclass---class_name-' |
      +-DBRpf-----+
      +-EXPort-----+
      |           .-DELETEDatest---No----- |
```

```

+-RPFfile--+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|           '-DELETEDatest--==+-No--+-' |
|           '-Yes-' |
|           .-DELETEDatest--==+-No-----' |
+-RPFSnapshot--+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|           '-DELETEDatest--==+-No--+-' |
|           '-Yes-' |
+-STGNew-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-STGReuse-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-STGDelete-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+'

```

Parámetros

TODate (Obligatorio)

Especifica la fecha a utilizar para seleccionar la información histórica de volúmenes secuenciales que se ha de suprimir. Solo puede suprimir los registros cuya fecha sea la misma o sea anterior a la fecha que especifique. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	01/23/1999
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-30 o -30. Para suprimir los registros con 30 días de antigüedad o más, puede especificar TODAY-30 o simplemente -30.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

TOTime

Especifica que desea suprimir los registros creados hasta esa hora inclusive en la fecha indicada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:30:22
NOW	La hora actual en la fecha especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada	NOW+03:00 o +03:00. Si emite el mandato DELETE VOLHISTORY a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect suprime los registros con la hora 12:00 o anterior en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada	NOW-03:30 o -03:30. Si emite el mandato DELETE VOLHISTORY a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect suprime los registros con la hora 5:30 o anterior en la fecha especificada.

Type (Necesario)

Especifica el tipo de los registros, que también cumplen los criterios de fecha y hora, que se suprimirán del archivo histórico de volúmenes. Los valores posibles son:

All

Especifica que se suprimirán todos los registros.

Restricción: El mandato DELETE VOLHISTORY no suprime los registros de los volúmenes remotos.

DBBackup

Especifica que sólo se suprimirán los registros que contienen información sobre los volúmenes utilizados para copias de seguridad incrementales y completas de la base de datos, es decir, con los tipos de volumen BACKUPFULL y BACKUPINCR, y que cumplen los criterios de fecha y hora especificados. No se suprimirán los registros de la última serie de copia de seguridad incremental y completa de la base de datos.

DEVclass=nombre_clase

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear copias de seguridad de la base de datos. Este parámetro opcional se puede utilizar para suprimir copias de seguridad de la base de datos creadas utilizando una clase de dispositivo de volúmenes virtuales de servidor a servidor. El tipo de clase de dispositivo debe ser SERVER. Este parámetro sólo se puede utilizar para suprimir entradas históricas de volumen del tipo BACKUPFULL, BACKUPINCR o DBSNAPSHOT.

Un volumen de copia de seguridad de base de datos completa o incremental puede seleccionarse para suprimirse si se cumplen todas las condiciones siguientes :

- La clase de dispositivo utilizada para crear el volumen de copia de seguridad de base de datos coincide con la clase de dispositivo especificada.
- El volumen se ha creado en la fecha y hora especificadas o antes.
- El volumen no forma parte de la serie de copias de seguridad de base de datos completa más incremental más reciente.
- El volumen no forma parte de una serie de copias de seguridad completa más incremental con una copia de seguridad de base de datos incremental creada después de una fecha y hora especificadas.

DBSnapshot

Especifica que sólo se suprimirán los registros que contienen información sobre los volúmenes utilizados para copias de seguridad de instantánea de base de datos y que cumplen los criterios de fecha y hora especificados. Los registros relacionados con la última copia de seguridad de base de datos de instantáneas no se suprimirán.

DEVclass=nombreclase

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear copias de seguridad de la base de datos. Este parámetro opcional se puede utilizar para suprimir copias de seguridad de la base de datos creadas utilizando una clase de dispositivo de volúmenes virtuales de servidor a servidor. El tipo de clase de dispositivo debe ser SERVER. Este parámetro sólo se puede utilizar para suprimir entradas históricas de volumen del tipo BACKUPFULL, BACKUPINCR o DBSNAPSHOT.

Un volumen de copia de seguridad de instantánea de base de datos puede seleccionarse para suprimirse si se cumplen todas las condiciones siguientes:

- La clase de dispositivo utilizada para crear el volumen de copia de seguridad de base de datos coincide con la clase de dispositivo especificada
- El volumen se ha creado en la fecha y hora especificadas o antes
- El volumen no forma parte de la última serie de copias de seguridad de base de datos de instantáneas

DBRpf

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos y los volúmenes de archivo del plan de recuperación.

EXPort

Especifica que sólo se suprimen los registros que contienen información sobre volúmenes de exportación.

RPFfile

Especifica que sólo se suprimen los registros que contienen información sobre los objetos de archivos del plan de recuperación que están almacenados en el servidor destino y que cumplen los criterios de fecha y hora especificados.

DELETEDatest

Especifica si el archivo del plan de recuperación más reciente es elegible para ser suprimido. Este parámetro opcional puede utilizarse para suprimir los archivos más recientes del plan de recuperación creados utilizando la clase de dispositivo de volúmenes virtuales de servidor a servidor.

Este parámetro sólo puede utilizarse para suprimir entradas históricas de volumen del tipo RPFfile (por ejemplo, los archivos del plan de recuperación creados con el parámetro DEVCLASS y el mandato PREPARE). Si no se especifica este parámetro, no se suprimirán las entradas RPFfile más recientes.

No

Especifica que el último archivo RPFfile no se suprime.

Sí

Especifica que el archivo RPFIL más reciente se suprime si cumple los criterios de fecha y hora especificados.

RPFSSnapshot

Especifica que sólo han de suprimirse los registros que contienen información acerca de los objetos de archivo de plan de recuperación que se han creado para las copias de seguridad de base de datos de instantáneas, que están almacenados en un servidor de destino y que cumplen los criterios de fecha y hora especificados. El último archivo RPFSSNAPSHOT no se eliminará a menos que cumpla los criterios de fecha y hora especificados y el parámetro DELETE se establezca en Yes.

DELETEDatest

Especifica si el archivo del plan de recuperación más reciente es elegible para ser suprimido. Este parámetro opcional puede utilizarse para suprimir los archivos más recientes del plan de recuperación creados utilizando la clase de dispositivo de volúmenes virtuales de servidor a servidor.

Este parámetro sólo puede utilizarse para suprimir entradas históricas de volumen del tipo RPFSSNAPSHOT (por ejemplo, los archivos del plan de recuperación creados con el parámetro DEVCLASS y el mandato PREPARE). Si no se especifica este parámetro, no se eliminarán las entradas RPFSSNAPSHOT más recientes.

No

Especifica que el último archivo RPFSSNAPSHOT no se suprime.

Sí

Especifica que el archivo RPFSSNAPSHOT más reciente se suprime si cumple los criterios de fecha y hora especificados.

STGNew

Especifica que sólo se suprimen los registros que contienen información sobre los nuevos volúmenes de almacenamiento de acceso secuencial.

STGReuse

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de almacenamiento de acceso secuencial reutilizados.

STGDelete

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de almacenamiento de acceso secuencial suprimidos.

Ejemplo: suprimir información de archivo de plan de recuperación

Suprimir toda la información del archivo de plan de recuperación que se crea en o antes del 28/03/2016.

```
delete volhistory type=rpfile todate=03/28/2016
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE VOLHISTORY

Mandato	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFIL	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.
SET DRMDBBACKUPEXPIREDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.

DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

Utilice este mandato para suprimir un volumen de agrupación de almacenamiento y, de forma opcional, los archivos almacenados en el volumen.

Si el volumen tiene datos, para suprimir el volumen debe hacer una de las posibilidades siguientes:

- Antes de suprimir el volumen, utilice el mandato MOVE DATA para traspasar todos los archivos a otro volumen.
- Solicite explícitamente que se descarten todos los archivos del volumen al suprimir el volumen (especificando DISCARDDATA=YES).

Si suprime varios volúmenes, debe suprimirlos de uno en uno. Si suprime varios volúmenes a la vez, el rendimiento del servidor puede resultar afectado de modo negativo.

No se pueden suprimir volúmenes de agrupación de almacenamiento si están utilizándose. Por ejemplo, no se puede suprimir un volumen si hay un usuario restaurando o recuperando un archivo que reside en el volumen, si el servidor está grabando información en el volumen o si hay un proceso de reclamación utilizando el volumen.

Si emite el mandato DELETE VOLUME, la información del volumen se suprime de la base de datos de IBM Spectrum Protect. Sin embargo, los archivos físicos que están asignados al mandato DEFINE VOLUME no se eliminan del espacio de archivos.

Si este mandato se aplica a un volumen WORM (una sola grabación, varias lecturas), el volumen se hará reutilizable si le queda espacio en el cual se pueden grabar datos. Los os datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el mandato CHECKOUT LIBVOLUME.

El mandato DELETE VOLUME actualiza automáticamente el inventario de bibliotecas del servidor correspondiente a los volúmenes secuenciales si el volumen vuelve a establecerse en el estado de reutilización cuando queda vacío. Para determinar si un volumen volverá al estado de reutilización, emita el mandato QUERY VOLUME y consulte la salida. Si el valor del atributo "¿Volumen reutilizable?" es "Sí", el inventario de bibliotecas del servidor se actualiza automáticamente.

Si el valor es "No," puede emitir el mandato UPDATE LIBVOLUME para especificar el estado de reutilización. Se recomienda emitir el mandato UPDATE LIBVOLUME después de haber emitido el mandato DELETE VOLUME.

El intento de utilizar el mandato DELETE VOLUME para suprimir volúmenes de WORM FILE de una agrupación de almacenamiento con RECLAMATIONTYPE=SNAPLOCK no se ejecuta correctamente y se genera un mensaje de error. La supresión de volúmenes de WORM FILE vacíos se realiza sólo a través del proceso de reclamación.

Si emite el mandato DELETE VOLUME para un volumen de una agrupación de almacenamiento que tiene un valor de parámetro SHRED mayor que 0, el volumen se establece en estado pendiente hasta que se ejecuta la destrucción. La destrucción es necesaria para que se complete la supresión, aunque el volumen esté vacío.

Si emite el mandato DELETE VOLUME para un volumen de una agrupación de almacenamiento configurada para la eliminación de datos duplicados, el servidor destruirá los objetos que hacen referencia a los datos de ese volumen.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento en la que está definido el volumen.

Sintaxis

```
.-DISCARDDATA-----No-----.  
>>-DELEte Volume--nombre_volumen--+-----+----->  
      '-DISCARDDATA-----+No--+ '  
                                '-Yes- '  
  
. -Wait-----No-----.  
>--+-----+-----><  
      '-Wait-----+No--+ '  
                                '-Yes- '
```

Parámetros

nombre_volumen (Necesario)

Especifica el nombre del volumen que se ha de suprimir.

DISCARDdata

Especifica si se suprimen los archivos almacenados en el volumen. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que no se suprimen los archivos almacenados en el volumen. Si el volumen contiene algún archivo, el volumen no se suprime.

Yes

Especifica que se suprimirán todos los archivos almacenados en el volumen. El servidor no necesita montar el volumen para este tipo de supresión.

Recuerde:

1. El servidor no suprime las copias archivadas que están en espera de supresión.
2. Si la protección de retención de archivado está activada, el servidor sólo suprime las copias archivadas cuyo período de retención ha caducado.

Si el volumen que se suprime es un volumen de agrupación de almacenamiento primaria, el servidor comprueba si alguna de las agrupaciones de almacenamiento de copia tiene copias de los archivos que se suprimen. Al suprimir los archivos almacenados en un volumen de agrupación de almacenamiento primaria, también se suprimen todas las copias que hay de esos archivos en las agrupaciones de almacenamiento de copia.

Al suprimir un volumen de disco de una agrupación de almacenamiento primaria, el mandato también suprime todos los archivos que son copias en caché (copias de los archivos que se han migrado a la siguiente agrupación de almacenamiento). Al suprimir en caché de los archivos no se suprimen los archivos que ya se han migrado o de los que se ha hecho una copia de seguridad en las agrupaciones de almacenamiento de copia. Solamente estarán afectadas las copias en caché de los archivos.

Si el volumen que se suprime es un volumen de agrupación de almacenamiento de copia, sólo se suprimen los archivos en el volumen de agrupación de copia. Los archivos de la agrupación de almacenamiento primaria no se verán afectados.

No utilice el mandato DELETE VOLUME con DISCARDdata=YES si está ejecutándose un proceso de restauración (RESTORE STGPPOOL o RESTORE VOLUME). El mandato DELETE VOLUME podría dar lugar a que la restauración no se completara.

Si cancela la operación DELETE VOLUME durante el proceso o si se produce un error del sistema, pueden que hayan quedado varios archivos en el volumen. Puede volver a suprimir el mismo volumen para que el servidor suprima los archivos que quedan y después el volumen.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro sólo afecta al proceso si también se ha solicitado que se descarten todos los datos del volumen. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Recuerde: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: suprimir un volumen de agrupación de almacenamiento

Suprimir el volumen de agrupación de almacenamiento stgvol.1 de la agrupación de almacenamiento FILEPOOL.

```
delete volume stgvol.1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DELETE VOLUME

Mandato	Descripción
---------	-------------

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

Mandatos DISABLE

Utilice los mandatos DISABLE para que el servidor no pueda realizar determinados tipos de operaciones.

- DISABLE EVENTS (Desactivar eventos para anotación de eventos)
- DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)
- DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)

DISABLE EVENTS (Desactivar eventos para anotación de eventos)

Utilice este mandato para desactivar el proceso de uno o varios eventos. Si especifica un receptor no admitido en ninguna plataforma o especifica un evento o nombre no válido, IBM Spectrum Protect emitirá un mensaje de error. Sin embargo, los receptores, eventos o nombres válidos que haya especificado seguirán habilitados.

Consejo: Los mensajes de la categoría SEVERE y el mensaje ANR9999D pueden proporcionar una valiosa información de diagnóstico si existen problemas graves en el servidor. Por este motivo, no debe desactivar estos mensajes.

Restricción:

- Determinados mensajes se visualizan en la consola incluso si están desactivados. Entre estos se encuentran algunos mensajes emitidos durante el proceso de arranque y conclusión del servidor y las respuestas a mandatos de administración.
- Los mensajes de servidor que se hayan originado en el servidor donde se ha emitido este mandato no se pueden desactivar para las anotaciones de actividades.

ANR1822I indica que las anotaciones de eventos se están finalizando para el receptor especificado. Cuando se emite el mandato DISABLE EVENTS este mensaje se anota en el receptor, aunque sea uno de los eventos que se han desactivado. Esto se hace para confirmar que las anotaciones de eventos han finalizado en ese receptor, pero los mensajes ANR1822I siguientes no se anotan en dicho receptor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .,-----
      v                                     |
>>-DISAbLe EVents-----+receivers-----+----->
      +-ALL-----+
      +-CONSOLE-----+
      +-ACTLOG-----+
      +-EVENTSERVER----+

```

```

++FILE-----+
++FILETEXT-----+
|           (1) |
++NTEVENTLOG-----+
|           (2) |
++SYSLOG-----+
++TIVOLI-----+
'-USEREXIT-----'

.-,-----
v |
>-----+nombre_evento+----->
++ALL-----+
++INFO-----+
++WARNING-----+
++ERROR-----+
'-SEVERE-----'

>+-----+-----><
|           .-,-----
|           v |
+-NODEname-----+nombre_nodo+-----+
|           .-,-----
|           v |
'-SERVERname-----+nombre_servidor+-----'

```

Notas:

1. NTEVENTLOG sólo está disponible en Windows.
2. SYSLOG sólo está disponible en Linux.

Parámetros

receptores (Obligatorio)

Especifica el nombre de los receptores cuyos eventos se desactivan. Especifique varios receptores separándolos con comas sin espacios intercalados. Los valores posibles son:

ALL

Todos los receptores, excepto los eventos del servidor en el receptor de anotaciones de actividades (ACTLOG). Para el receptor de anotaciones de actividades únicamente se pueden desactivar los eventos de clientes.

CONSOLE

La consola estándar del servidor como receptor.

ACTLOG

Las anotaciones de actividades como receptor. Sólo puede desactivar los eventos de cliente, no los eventos de servidor, para las anotaciones de actividades.

EVENTSERVER

El servidor de eventos como receptor.

FILE

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo. Los registros no pueden ser leídos fácilmente por cualquier persona.


FILETEXT

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

NTEVENTLOG

Las anotaciones de aplicaciones de Windows como receptor.

Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEscribe mensajes directamente al registro del sistema en Linux.

TIVOLI

Tivoli Enterprise Console (TEC) como receptor.

USEREXIT

Un programa escrito por el usuario como receptor. El servidor escribe información en el programa.

sucesos (Obligatorio)

Especifica los eventos que se desactivan. Puede especificar varios eventos separándolos con comas sin espacios intercalados. Los valores posibles son:

ALL

Todos los eventos.

nombre_evento

Un número de mensaje de cuatro dígitos que tiene antepuesto **ANR** para un evento del servidor o **ANE** para un evento del cliente. Los rangos válidos son de ANR0001 a ANR9999 y de ANE4000 a ANE4999. Especifique el parámetro **NODENAMES** si los eventos del cliente se van a desactivar para los nodos coincidentes. Especifique el parámetro **SERVERNAME** si los eventos del servidor se van a desactivar para los servidores coincidentes.

Sólo para el receptor de eventos de **TIVOLI**, puede especificar los siguientes nombres de eventos para los clientes de la aplicación **IBM Spectrum Protect**:

cliente de aplicaciones de IBM Spectrum Protect	Prefijo	Rango
Data Protection para Microsoft Exchange Server	ACN	3500–3649
Data Protection para Lotus Domino	ACD	5200–5299
Data Protection para Oracle	ANS	500–599
Data Protection para Informix	ANS	600–699
Data Protection para Microsoft SQL Server	ACO	3000–3999

Recuerde: Si se especifica **ALL** se desactivan estos mensajes. Sin embargo, las opciones **INFO**, **WARNING**, **ERROR** y **SEVERE** no tienen ningún efecto sobre los mensajes.

categorias de gravedad

Si la lista de eventos contiene una categoría de gravedad, todos los eventos de dicha gravedad se desactivarán para los nodos especificados. Los tipos de mensajes son:

INFO

Mensajes informativos (de tipo I).

WARNING

Mensajes de aviso (de tipo W).

ERROR

Mensajes de error (de tipo E).

SEVERE

Mensajes de error grave (de tipo S).

NODENAME

Especifica el nombre de uno o varios nodos cuyos eventos se desactivan. Puede utilizar el carácter comodín (*) para especificar todos los nodos. Puede especificar **NODENAME** o **SERVERNAME**. Si no se especifica ninguno de los parámetros, los eventos se desactivan para el servidor donde se ejecuta este mandato.

SERVERNAME

Especifica el nombre de uno o varios servidores cuyos eventos se desactivan. Puede utilizar el carácter comodín (*) para especificar todos los servidores excepto el servidor donde se ejecuta este mandato. Puede especificar **NODENAME** o **SERVERNAME**. Si no se especifica ninguno de los parámetros, los eventos se desactivan para el servidor donde se ejecuta este mandato.

Ejemplo: desactivar categorías específicas de eventos

Desactivar todos los eventos de clientes de las categorías **INFO** y **WARNING** para las anotaciones de actividad y receptores de consola para todos los nodos.

```
disable events actlog,console
info,warning nodename=*
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con **DISABLE EVENTS**

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET .

DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)

Utilice este mandato para impedir que un servidor de réplica de origen inicie nuevos procesos de réplica.

El uso de este mandato no detiene la ejecución de procesos de réplica. La ejecución de procesos de réplica continuará hasta que se completen o hasta que finalicen sin completarse. Utilice este mandato y el mandato ENABLE REPLICATION para controlar el proceso de réplica.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-DISAbLe REPLiCation-----><
```

Parámetros

Ninguno.

Ejemplo: desactivar el proceso de réplica

Desactive el proceso de réplica en un servidor de réplica de origen.

```
disable replication
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DISABLE REPLICATION

Mandato	Descripción
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)

Utilice este mandato para impedir el acceso de nuevas sesiones a IBM Spectrum Protect. Las sesiones activas se completarán. Para un determinado servidor, puede especificar si se desactivan las sesiones de entrada, las sesiones de salida o ambas.

Los procesos del servidor como, por ejemplo, operaciones de migración y reclamación, no resultan afectadas cuando se emite el mandato DISABLE SESSIONS.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```
>>-DISAbLe SESSions----->
.-CLient-----.
>--+-----+><
'|++CLient-----|'
'|++ALL-----+'
'|++ADMin-----+'
'|'-SERVer-----+'
'|
|      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
'|-nombre_servidor-----+'
'|      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
'|++-DIRectioN-----Both-----+'
'|++-DIRectioN-----INbound-----+'
'|--DIRectioN-----OUTbound-----|'
```

Parámetros

Especifica el tipo de sesión que se desactiva. Este parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

CLient

Inhabilita sólo las sesiones de cliente de copia de seguridad y archivado.

ALL

Inhabilita todos los tipos de sesión.

ADMin

Inhabilita sólo las sesiones administrativas.

SERVer

Inhabilita sólo las sesiones de servidor a servidor. Sólo se desactivan los siguientes tipos de sesiones:

- Anotación de eventos de servidor a servidor
- Gestión empresarial
- Inscripción servidor
- Fuera de la LAN: almacenamiento agente - servidor
- Volúmenes virtuales
- Réplica de nodo

También puede especificar si se desactivan las sesiones de entrada, las sesiones de salida o ambas para un determinado servidor.

nombre_servidor

Especifica el nombre del servidor cuyas sesiones desea desactivar. Este parámetro es opcional. Si no especifica este parámetro, no se inician nuevas sesiones con otros servidores. Las sesiones en ejecución no se cancelan.

DIRectioN

Especifica si se desactivan las sesiones de entrada, las sesiones de salida o ambas. Este parámetro es opcional. El valor predeterminado es BOTH. Son posibles los siguientes valores:

Both

Especifica que se desactivan las sesiones de entrada desde el servidor especificado y las sesiones de salida hacia el servidor especificado.

INbound

Especifica que sólo se desactivan las sesiones de entrada desde el servidor especificado.

OUTbound

Especifica que sólo se desactivan las sesiones de salida hacia el servidor especificado.

Ejemplo: impedir que se establezcan nuevas sesiones de copia de seguridad y archivado de nodo cliente en el servidor

Impedir temporalmente que nuevas sesiones de nodos clientes accedan al servidor.

```
disable sessions
```

Ejemplo: impedir que puedan establecerse nuevas sesiones en el servidor

Impedir temporalmente que nuevas sesiones accedan al servidor.

```
disable sessions all
```

Ejemplo: desactivar las sesiones de salida hacia un servidor

Desactive las sesiones de salida hacia un servidor denominado REPLSRV.

```
disable sessions server replsrv direction=outbound
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DISABLE SESSIONS

Mandato	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

Mandatos DISMOUNT

Utilice el mandato DISMOUNT para desmontar un volumen mediante la dirección de dispositivo real o mediante el nombre de volumen.

- DISMOUNT VOLUME (Desmontar un volumen por nombre de volumen)

DISPLAY OBJNAME (Mostrar un nombre de objeto completo)

Utilice este mandato para IBM Spectrum Protect que se visualice un nombre de objeto completo si el nombre que figura en un mensaje o en la salida de una consulta está abreviado por razones de limitación de longitud. Los nombres de objeto que son muy largos pueden ser difíciles de mostrar y usar en funciones normales del sistema operativo. El servidor IBM Spectrum Protect abreviará nombres largos y les asignará un ID de señal que puede utilizarse si el nombre de la ruta del objeto sobrepasa los 1024 bytes. El ID de señal se muestra en una cadena que incluye identificadores para el nodo, el espacio de archivos y el nombre del objeto. El formato es: [TSMOBJ:nID.fsID.objID]. Cuando se especifica con el mandato DISPLAY OBJNAME, el ID de señal puede utilizarse para que se muestre el nombre completo del objeto.

Clase de privilegio

Cualquier administrador puede emitir este mandato

Sintaxis

```
>>-DISplay OBJname--ID_ñeñal-----<<
```

Parámetros

ID_ñeñal (Necesario)

Especifica el ID que se indica en la etiqueta [TSMOBJ:], cuando el nombre de un objeto es demasiado largo para mostrarlo.

Ejemplo: visualizar el nombre de objeto completo de un ID de señal en un mensaje

Supongamos que se recibe el mensaje siguiente:

```
ANR9999D file.c(1999) Error al manejar archivo [TSMOBJ:1.1.649498]  
debido a la falta de recursos de servidor.
```

Para mostrar el nombre de objeto completo del archivo al que se hace referencia en el mensaje de error, especifique el ID de señal en el mandato DISPLAY OBJNAME.

Mandatos relacionados

Tabla 1. Mandatos relacionados con DISPLAY OBJNAME

Mandato	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.

Mandatos ENABLE

Utilice el mandato ENABLE para que el servidor pueda realizar algunos tipos de operaciones.

- ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)
- ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)
- ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)

ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)

Utilice este mandato para activar el proceso de uno o varios eventos. Si especifica un receptor no admitido en ninguna plataforma o especifica un evento o nombre no válido, IBM Spectrum Protect emitirá un mensaje de error. Sin embargo, los receptores, eventos o nombres válidos que haya especificado seguirán habilitados.

Restricción: Algunos eventos, como algunos mensajes emitidos durante el arranque o la conclusión del servidor, van directamente a la consola. No van a otros receptores aunque estén activados.

Los mandatos de administración se devuelven al emisor del mandato y sólo se registran como sucesos numerados. Estos sucesos numerados no se registran en la consola del sistema, pero sí en los demás receptores, incluidas las sesiones de línea de mandatos de administración que se ejecutan en modalidad de consola.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-,-----
      v                               |
>>-ENable--EEvents---+--ALL-----+----->
                        +-CONSOLE-----+
                        +-ACTLOG-----+
                        +-EVENTSERVER----+
                        +-FILE-----+
                        +-FILETEXT-----+
                        |               (1) |
                        +-NTEVENTLOG----+
                        |               (2) |
                        +-SYSLOG-----+
                        +-TIVOLI-----+
                        '-USEREXIT-----'

      .-,-----
      v                               |
>---+--nombre_evento--+----->
      +-ALL-----+
      +-INFO-----+
      +-WARNING-----+
      +-ERROR-----+
      '-SEVERE-----'

>---+-----<
      |               .-,-----
      |               v                               |
      +-NODEname-----+--nombre_nodo+-----+

```

```

| .-,-,----- . |
| v | |
| '-SERVname--==-----nombre_servidor--+-'

```

Notas:

1. NTEVENTLOG sólo está disponible en Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

Parámetros

receptores (Obligatorio)

Especifica uno o varios receptores para los que se anotan los eventos activados. Puede especificar varios receptores separándolos con comas sin espacios intercalados. Los valores válidos son:

ALL

Todos los receptores.

CONSOLE

La consola estándar del servidor como receptor.

ACTLOG

Las anotaciones de actividades del servidor como receptor.

EVENTSERVER


El servidor de eventos como receptor.


FILE


Un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo. Los registros no pueden ser leídos fácilmente por cualquier persona.


FILETEXT

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos Windows NTEVENTLOG

 Sistemas operativos Windows Las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos Linux SYSLOG

 Sistemas operativos Linux Especifica el registro de sistema de Linux como receptor.

TIVOLI

Tivoli Enterprise Console (TEC) como receptor.

USEREXIT

Un programa escrito por el usuario como receptor. El servidor escribe información en el programa.

sucesos (Obligatorio)

Especifica el tipo de eventos que se activan. Puede especificar varios eventos separándolos con comas sin espacios intercalados. Los valores posibles son:

ALL

Todos los eventos.

nombre_evento

Un número de mensaje de cuatro dígitos que tiene antepuesto ANR para un evento del servidor o ANE para un evento del cliente. Los rangos válidos son de ANR0001 a ANR9999 y de ANE4000 a ANE4999. Especifique el parámetro NODENAME si los eventos del cliente se van a activar para nodos coincidentes. Especifique el parámetro SERVERNAME si los eventos del servidor se van a activar para los servidores coincidentes.

Para el receptor de eventos de TIVOLI, puede especificar los siguientes rangos adicionales para los clientes de la aplicación IBM Spectrum Protect:

cliente de aplicaciones de IBM Spectrum Protect	Prefijo	Rango
Data Protection para Microsoft Exchange Server	ACN	3500–3649
Data Protection para Lotus Domino	ACD	5200–5299
Data Protection para Oracle	ANS	500–599
Data Protection para Informix	ANS	600–699
Data Protection para Microsoft SQL Server	ACO	3000–3999

Restricción: El cliente de aplicación debe tener activado el soporte para Tivoli Event Console ampliado con el fin de poder direccionar estos mensajes a Tivoli Event Console.

Consejo:

- Si se especifica la opción ALL se activan estos mensajes. Sin embargo, las opciones INFO, WARNING, ERROR y SEVERE no tienen ningún efecto sobre los mensajes.
- Debido al número de mensajes, no se deben activar todos los mensajes de un nodo para que se anoten en Tivoli Event Console.

categorias de gravedad

Si la lista de eventos contiene una categoría de gravedad, todos los eventos de dicha gravedad se activarán para los nodos especificados. Los tipos de mensajes son:

INFO

Se activan los mensajes informativos (de tipo I).

WARNING

Se activan los mensajes de aviso (de tipo W).

ERROR

Se activan los mensajes de error (de tipo E).

SEVERE

Se activan los mensajes de error grave (de tipo S).

NODENAME

Especifica uno o varios nodos cliente para los que se activan los eventos. Puede utilizar un carácter comodín para especificar todos los nodos cliente. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, los eventos se activan para el servidor donde se ejecuta este mandato.

SERVRNAME

Especifica uno o varios servidores para los que se activan los eventos. Puede utilizar un carácter comodín para especificar todos los servidores excepto el servidor donde se ejecuta este mandato. Puede especificar SERVERNAME o NODENAME. Si no se especifica ninguno de los parámetros, los eventos se activan para el servidor donde se ejecuta este mandato.

Ejemplo: activar categorías específicas de eventos

Activar todos los eventos del cliente ERROR y SEVERE para el receptor USEREXIT y el nodo BONZO.

```
enable events userexit error,severe nodename=bonzo
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ENABLE EVENTS

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)

Utilice este mandato para permitir que un servidor de réplica de origen inicie el proceso de réplica normal después de una restauración de base de datos. También puede utilizar este mandato para reanudar el proceso de réplica después de emitir el mandato DISABLE REPLICATION.

Atención: Antes de activar la réplica después de una restauración de base de datos, determine si las copias de los datos que hay en el servidor de destino son necesarias. Si lo son, debe sincronizar los datos del nodo de cliente replicando los datos del servidor de réplica de destino en el servidor de réplica de origen. El proceso de réplica sustituye los datos en el servidor de origen que se han perdido debido a la restauración de base de datos.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-ENable REPLication-----<<
```

Parámetros

Ninguno.

Ejemplo: permitir el proceso de réplica

Permita el proceso de réplica en un servidor de réplica de origen.

```
enable replication
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ENABLE REPLICATION

Mandato	Descripción
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)

Utilice este mandato después de emitir el mandato DISABLE SESSIONS para iniciar nuevas sesiones que puedan acceder a un servidor. Para un determinado servidor, puede especificar si se activan las sesiones de entrada, las sesiones de salida o ambas.

El proceso de este mandato no afecta a los procesos del sistema como por ejemplo, migración y reclamación.

Utilice el mandato QUERY STATUS para visualizar la disponibilidad del servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```
>>-ENable SESSions----->
.-CLient-----
>--+-----+><
'|+-CLient-----+'
  +-ALL-----+
  +-ADMin-----+
  '-SERVer--+-----+'
      |               .-DIRection--==Both-----|
      '-nombre_servidor--+-----+'
      '+-DIRection--==Both-----+'
      '+-DIRection--==INbound--+-----'
```

Parámetros

Especifica el tipo de sesión que se activa. Este parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

CLient

Habilita sólo las sesiones de cliente de copia de seguridad y archivado.

ALL

Habilita todos los tipos de sesión.

ADMin

Habilita sólo las sesiones administrativas.

SERVer

Habilita sólo las sesiones de servidor a servidor. También puede especificar si se activan las sesiones de entrada, las sesiones de salida o ambas para un determinado servidor.

nombre_servidor

Especifica el nombre de un determinado servidor cuyas sesiones desea activar. Este parámetro es opcional. Si no especifica este parámetro, se activan nuevas sesiones con los demás servidores.

DIRection

Especifica si se activan las sesiones de entrada, las sesiones de salida o ambas. Este parámetro es opcional. El valor predeterminado es BOTH. Son posibles los siguientes valores:

Both

Especifica que se activan las sesiones de entrada desde el servidor especificado y las sesiones de salida hacia el servidor especificado.

INbound

Especifica que sólo se activan las sesiones de entrada hacia el servidor especificado.

OUTbound

Especifica que sólo se activan las sesiones de salida desde el servidor especificado.

Ejemplo: reanudar la actividad del nodo cliente en el servidor

Reanudar la operación normal, permite a los nodos clientes acceder al servidor.

```
enable sessions
```

Ejemplo: reanudar todas las actividades en el servidor

Reanudar la operación normal, permite a todas las sesiones acceder al servidor.

```
enable sessions all
```

Ejemplo: activar las sesiones de salida hacia un servidor

Active las sesiones de salida hacia un servidor denominado REPLSRV.

```
enable sessions server replsrv direction=outbound
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ENABLE SESSIONS


Mandato	Descripción
ACCEPT DATE	Acepta la fecha actual en el servidor.
CANCEL SESSION	Cancela las sesiones activas con el servidor.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.


FILE


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

Ejemplo: detener las anotaciones de eventos

Finalizar la anotación de eventos en la salida de usuario.

```
end eventlogging userexit
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con END EVENTLOGGING

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)

Utilice este mandato para iniciar manualmente el proceso de caducidad de inventario. El proceso de caducidad de inventario elimina las copias de los archivos de archivado y de copia de seguridad de cliente del almacenamiento del servidor. La eliminación se basa en las especificaciones de política de los grupos de copia de archivado y de copia de seguridad y archivo de las clases de gestión a las que están vinculados los archivos.

Si tiene la función de gestor de recuperación ante siniestro para el servidor de IBM Spectrum Protect, el proceso de caducidad de inventario también elimina los volúmenes virtuales elegibles que se utilizan para los procesos siguientes:

- Copias de seguridad de base de datos del tipo BACKUPFULL, BACKUPINCR y DBSNAPSHOT. El mandato SET DRMDBBACKUPEXPIREDAYS controla cuándo podrán seleccionarse estos volúmenes para su caducidad.
- Archivos del plan de recuperación del tipo RPFILe y RPFNSAPSHOT. El mandato SET DRMRPFEXPIREDAYS controla cuándo podrán seleccionarse estos volúmenes para su caducidad.

El proceso de caducidad de inventario que se ejecuta durante la inicialización del servidor no elimina estos volúmenes virtuales.

Tan solo se permite un proceso de caducidad a la vez, pero este proceso se puede distribuir entre un máximo de 40 hebras. Si hay un proceso de caducidad en ejecución, no puede iniciar otro proceso.

Puede configurar el proceso de caducidad automático con la opción de servidor EXPINTERVAL. Si establece la opción EXPINTERVAL en 0, el servidor no ejecutará automáticamente el proceso de caducidad y deberá emitir el mandato EXPIRE INVENTORY para iniciar el proceso.

Este mandato crea un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Si se aplica este mandato a un volumen WORM, el volumen vuelve a ser un volumen cero si hay espacio restante en el que se pueden escribir los datos. Los os datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el mandato CHECKOUT LIBVOLUME.

Ejecute el mandato EXPIRE INVENTORY para suprimir archivos del almacenamiento del servidor si no se ha suprimido cuando utilizó las operaciones de supresión del cliente.

Si desea más información sobre las operaciones de supresión de cliente, consulte Mandatos y opciones de cliente de archivado y copia de seguridad.

Clase de privilegio

Para emitir este mandato, debe tener privilegios de sistema.

Sintaxis

```
.-Quiet---No-----
>>-EXPIre Inventory----->
'-Quiet---+No---+'
          '-Yes-'

.-Wait---No----- .-Nodes---*-----
>----->
'-Wait---+No---+' '-Nodes---+nombre_nodo-----+'
          '-Yes-'          '-nombre_grupo_nodos-'

>----->
'-EXCLUDENodes---nombre_nodo_excluido-'

.-Type---All-----
>----->
'-Domain---domain_name-' '-Type---+All-----+'
          +-Archive+
          +-Backup--+
          '-Other--'

.-REsource---4----- .-Skipdirs---No-----
>----->
'-REsource---numero-' '-Skipdirs---+No---+'
          '-Yes-'

>-----<
'-Duration---minutos-'
```

Parámetros

Quiet

Especifica si el servidor ha de suprimir los mensajes detallados relativos a cambios de políticas durante el proceso de caducidad. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor envía mensajes informativos detallados.

Yes

Especifica que el servidor sólo envía mensajes resumidos. El servidor emite mensajes acerca de los cambios de política únicamente cuando se suprimen los archivos y cuando se utilizó la clase de gestión predeterminada o el periodo de gracia de retención para el dominio para caducar los archivos.

También puede especificar la opción EXPQUIET del archivo de opciones del servidor para determinar automáticamente si el proceso de caducidad se ejecuta con mensajes resumidos.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

SKIPDIRS

Especifica si el servidor omite los objetos tipo directorio durante el proceso de caducidad. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor caduca los archivos y directorios según los criterios de la política correspondiente.

Yes

Especifica que el servidor omite los objetos tipo directorio y los objetos de archivado durante el proceso de caducidad, aunque los directorios se puedan seleccionar para la caducidad. Si especifica YES, impedirá que se supriman los directorios y el proceso de caducidad puede llevarse a cabo con más rapidez.

Atención: No utilice esta opción todo el tiempo. Con IBM Spectrum Protect Versión 6.0 y posteriores, puede ejecutar varias hebras (recursos) para un proceso de caducidad. Asimismo, si especifica YES con frecuencia, el tamaño de la base de datos aumenta a medida que se acumulan los objetos de directorio y aumenta el período de tiempo utilizado para la caducidad. Ejecute SKIPDIRS=NO periódicamente para que caduquen los directorios y disminuya el tamaño de la base de datos.

Nodes

Especifica el nombre de los nodos cliente y de los grupos de nodos cuyos datos van a procesarse. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Este parámetro es opcional.

Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de mandato NODES y DOMAIN, y que no coincidan con los criterios para las opciones de mandato EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

EXCLUDENodes

Especifica el nombre de los nodos de cliente y de los grupos de nodos cuyos datos no van a procesarse. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Este parámetro es opcional.

Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de mandato NODES y DOMAIN, y que no coincidan con los criterios para las opciones de mandato EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

Domain

Especifica que solo van a procesarse los datos para los nodos de cliente asignados al dominio especificado. Este parámetro es opcional. Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de mandato NODES y DOMAIN, y que no coincidan con los criterios para las opciones de mandato EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

Type

Especifica el tipo de datos que se van a procesar. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

ALL

Procesa todos los tipos de datos que pueden elegirse para la caducidad.

Archive

Procesa solo los datos de archivado de cliente.

Backup

Procesa solo los datos de copia de seguridad de cliente.

Otro

Procesa solo los elementos para las funciones del gestor de recuperación ante siniestro, como los archivos del plan de recuperación y copias de seguridad de bases de datos obsoletas.

REsource

Especifica el número de hebras que se pueden ejecutar en paralelo. Especifique un valor en el rango de 1 a 40. Este parámetro es opcional. El valor predeterminado es cuatro.

La caducidad se ejecuta como un proceso único, aunque los recursos representan el trabajo en paralelo por parte del servidor dentro del proceso de caducidad único. Los datos de archivado de un nodo sólo se ejecutan en un único recurso, pero los datos de copia de seguridad se puede propagar entre recursos de un nivel de espacio de archivos. Por ejemplo, si especifica `NODE=X, Y, Z` cada uno con tres espacios de archivos y `RESOURCE=5`, el proceso de caducidad para los tres nodos de cliente X, Y y Z se ejecuta en paralelo. Al menos un recurso procesa cada nodo y, al menos, un nodo utiliza múltiples recursos para procesar datos de copia de seguridad entre los distintos espacios de archivo.

DUration

Especifica el número máximo de minutos que debe esperarse a que se ejecute el proceso de caducidad. El proceso se detiene cuando transcurre el número de minutos especificado o cuando se han suprimido todos los objetos caducados seleccionables, lo que ocurra primero. Especifique un valor en el rango de 1 a 2880. Este parámetro es opcional. Si este parámetro no se especifica, la duración del proceso de caducidad no queda limitado por la hora.

Ejemplo: ejecutar el proceso de caducidad de inventario para un período de tiempo específico

Ejecutar el proceso de caducidad en un plazo de dos horas.

```
expire inventory duration=120
```

Ejemplo: ejecutar el proceso de caducidad de inventario para los datos de copia de seguridad para dos nodos cliente

Ejecutar el proceso de caducidad de inventario para los datos de copia de seguridad para dos nodos cliente, CHARLIE y ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory nodes=charlie,robbie resource=2 type=backup
```

Ejemplo: ejecutar el proceso de caducidad de inventario para todos los nodos de cliente excepto dos nodos

Ejecute el proceso de caducidad de inventario para todos los nodos de cliente, excepto dos nodos, CHARLIE y ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory excludenodes=charlie,robbie
```

Ejemplo: ejecutar el proceso de caducidad de inventario para todos los nodos de cliente en un dominio, excepto un nodo

Ejecute el proceso de caducidad de inventario para todos los nodos de cliente en un dominio, excepto un nodo, ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory domain=standard excludenodes=robbie
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con EXPIRE INVENTORY

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
CANCEL EXPIRATION	Cancela el proceso de caducidad de inventario.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.

Mandatos EXPORT

Utilice el mandato EXPORT para copiar información de un servidor de IBM Spectrum Protect en un medio extraíble secuencial.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

- EXPORT ADMIN (Exportar información del administrador)
- EXPORT NODE (Exportar información de nodos cliente)
- EXPORT POLICY (Exportar información de políticas)
- EXPORT SERVER (Exportar información del servidor)

EXPORT ADMIN (Exportar información del administrador)

Utilice este mandato para exportar definiciones de administrador y de autorización desde un servidor. Se puede exportar la información a medios secuenciales para después importarla a otro servidor, o bien se puede exportar la información directamente a otro servidor para su importación inmediata.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

IBM Spectrum Protect exporta información de administrador como, por ejemplo:

- El nombre, la contraseña y la información de contacto del administrador
- Clases de privilegios de administración que se otorgan al administrador
- Si el ID de administrador tiene bloqueado el acceso del servidor

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de exportación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si exporta información a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

El mandato EXPORT ADMIN ofrece dos posibilidades: exportación directa a otro servidor de la red o bien exportación a un medio secuencial. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con EXPORT ADMIN

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

- EXPORT ADMIN (Exportar definiciones del administrador a medios secuenciales)
Se pueden exportar definiciones de administrador y de autorización de un servidor a un medio secuencial para después importarlas a otro servidor.
- EXPORT ADMIN (Exportar información del administrador directamente a otro servidor)
Utilice este mandato para exportar definiciones de administrador y de autorización directamente a otro servidor de la red. Así se genera una importación inmediata en el servidor de destino.

EXPORT ADMIN (Exportar definiciones del administrador a medios secuenciales)

Se pueden exportar definiciones de administrador y de autorización de un servidor a un medio secuencial para después importarlas a otro servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.-*-----
>>-EXPort Admin----->
      | .-,-----|
      | V          |
      |'---nombre_admin---'|

.-Preview ----No-----
>+----->
|          (1) (2)          |
|'-Preview-----+No---+-'|
|                          |'-Yes-'|

>+----->
|          (1)          |
|'-DEVclass-----nombre_clase_dispositivo-'|










.-Scratch----Yes-----
>+----->
|          (2)          |
|'-Scratch-----+Yes---+-'|
|                          |'-No--'|

>+----->
|          (2)          |
|          V          |
|'-VOLumenames-----+nombre_volumen---+-'|
|                          |'-FILE:--nombre_archivo-'|

>+----->
|'-USEDVolumelist----nombre_archivo-'

```


Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el mandato emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

Ejemplo: exportar definiciones de administrador a volúmenes de cinta

Desde el servidor, exportar la información de todos los administradores definidos a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Se informa sobre el número y tipo de los objetos a la consola del sistema y a las anotaciones de actividades. Emita el mandato:

```
export admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Ejemplo: exportar definiciones de administrador a volúmenes de cinta listados en un archivo

Desde el servidor, exporte la información para todos los administradores definidos en los volúmenes de cintas que figuran en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA

Este archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export admin devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export admin devclass=menu1 volumenames=file:tapevol.data
```

Se informa sobre el número y tipo de los objetos a la consola del sistema y a las anotaciones de actividades.

EXPORT ADMIN (Exportar información del administrador directamente a otro servidor)

Utilice este mandato para exportar definiciones de administrador y de autorización directamente a otro servidor de la red. Así se genera una importación inmediata en el servidor de destino.

Puede emitir el mandato QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
.-*----->
>>-EXPort Admin--+----->
| .,-----|
| V         |
|---nombre_admin---|
>--+----->
'-TOServer----nombre_servidor-'
. -PREVIEWImport----No----- . -Replacedefs----No-----
>--+----->
'-PREVIEWImport----+No--+-' '-Replacedefs----+No--+-'
          '-Yes-'          '-Yes-'
. -ENCryptionstrength----AES-----
>--+----->
'-ENCryptionstrength----+AES--+-'
          '-DES-'
```

Parámetros

nombre_admin

Especifica los administradores para los que se va a exportar la información. Este parámetro es opcional. El valor predeterminado son todos los administradores.

Debe separar los elementos de la lista con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el mandato DEFINE SERVER. El administrador que emita el mandato de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES.

Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

Ejemplo: exportar las definiciones del administrador a un servidor de destino

Exportar todas las definiciones de administrador al servidor destino definido como OTHERSERVER. Previsualizar las operaciones de importación en el servidor destino. Emita el mandato:

```
export admin * toserver=otherserver previewimport=yes
```

Desde el servidor de destino, OTHERSERVER, puede visualizar las operaciones de importación si emite el mandato:

```
proceso de consulta
```

EXPORT NODE (Exportar información de nodos cliente)

Utilice este mandato para exportar definiciones de nodos cliente o datos de archivos a medios secuenciales o directamente a otro servidor para su importación inmediata.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

La siguiente información se incluye en cada definición de nodo cliente:

- El ID de usuario, la contraseña y la información de contacto.
- El nombre del dominio de políticas asignado del cliente.
- El estado de compresión de archivos.
- Si el usuario tiene autorización para suprimir copias de seguridad o copias archivadas del almacenamiento del servidor.
- Si el ID de nodo cliente tiene bloqueado el acceso al servidor.

De forma opcional, también puede exportar los elementos siguientes:

- Definiciones de espacio de archivos.
- Copias de seguridad, copias archivadas y archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.
- Información de autorización de acceso que pertenece a los espacios de archivos exportados.
- Los datos de copia archivada cuyo estado es en espera de supresión (dicho estado se conservará). Cuando los datos de copia archivada se importan, permanecerán en espera de retención.

Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores a los que se exportan deben estar configurados para las contraseñas de LDAP. Los datos del nodo que se exportan desde un nodo que se autentica con un servidor de directorios LDAP no son accesible si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos exportados desde un nodo de LDAP todavía se pueden exportar. Pero el servidor de destino debe estar configurado para utilizar LDAP, para acceder a los datos.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.
- Los mandatos EXPORT NODE y EXPORT SERVER no exportan datos de una agrupación de fragmentación a menos que lo permita de forma explícita estableciendo el parámetro ALLOWSHREDDABLE en el valor YES. Si se especifica este valor y los datos exportados incluyen datos de agrupaciones de destrucción, esos datos no se podrán destruir. No se emite ningún aviso si la operación de exportación incluye datos de agrupaciones de fragmentación.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
 - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.
 - Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
 - Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESPPACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

El mandato EXPORT NODE genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si está exportando información de nodo a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Para visualizar información sobre cualquiera de las opciones de exportación de servidor a servidor suspendidas o en ejecución, emita el mandato QUERY EXPORT. El mandato QUERY EXPORT sólo visualiza información acerca de las exportaciones que se han suspendido o que pueden suspenderse. Las operaciones de exportación que pueden suspenderse, y reiniciarse posteriormente, son las exportaciones de servidor a servidor cuyo FILEDATA tiene un valor distinto de NONE. Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de exportación.

Dado que pueden producirse resultados imprevisibles, no ejecute procesos de caducidad, migración, copia de seguridad o archivado cuando emita el mandato EXPORT NODE.

Para un servidor que tenga clientes que admitan Unicode, puede conseguir que el servidor convierta el nombre de espacio de archivos que especifique, o bien utilizar uno de los parámetros siguientes:

- FSID
- UNIFILESPACE

El mandato EXPORT NODE ofrece dos posibilidades: exportación directa a otro servidor de la red o bien exportación a un medio secuencial. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con EXPORT NODE

Mandato	Descripción
---------	-------------

Mandato	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

- EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)
Se pueden exportar definiciones de nodo o datos de archivos de un servidor a un medio secuencial para después importarlas a otro servidor.
- EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)
Utilice este mandato para exportar definiciones de nodos cliente o datos de archivos directamente a otro servidor para su importación inmediata.

EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)

Se pueden exportar definiciones de nodo o datos de archivos de un servidor a un medio secuencial para después importarlas a otro servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.-*-----
>>-EXPoRT Node----->
| .-,-----|
| v         | |
|'---nombre_nodo+-'
>----->
| .-,-----|
| v         | |
|'-FILESpace-----nombre_espacio_archivos+-'
>----->
| .-,-----|
| v         | |
|'-FSID-----ID_espacio_archivos+-'
>----->
| .-,-----|
| v         | |
|'-UNIFILESpace-----nombre_espacio_archivos+-'
>----->
| .-,-----|

```


FILESpace

Especifica los espacios de archivos para los que se van a exportar los datos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

Restricción: Si se especifica un espacio de archivos, los espacios de archivos habilitados para Unicode no se exportan.

FSID

Especifica los espacios de archivos utilizando sus identificadores de espacios de archivos (FSID). El servidor utiliza los identificadores FSID para encontrar los espacios de archivos que se deben exportar. Para buscar el FSID para un espacio de archivos, utilice el mandato QUERY FILESPACE. Puede separar varios identificadores de espacios de archivos con comas y sin espacios intercalados. Este parámetro es opcional.

UNIFILESpace

Especifica los espacios de archivos que el servidor reconoce como activados para Unicode. El servidor convierte los nombres entrados de la página de códigos del servidor a la página de códigos UTF-8 para encontrar los espacios de archivos a exportar. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizarse un carácter comodín para especificar un nombre. Este parámetro es opcional.

DOmains

Especifica los dominios de políticas desde donde deben exportarse los nodos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Si especifica dominios, sólo se exportarán los nodos si pertenecen a uno de los dominios especificados. Puede utilizar caracteres comodín para especificar un nombre.

FILEData

Especifica el tipo de archivos que se deben exportar para todos los nodos que se están exportando al servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Nota: Si está exportando un nodo que tiene datos de grupo, los datos que no son parte de los objetos de destino podrían exportarse. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. Por ejemplo, si FILEDATA=BACKUPACTIVE cuando se especifican los parámetros FROMDATE o TODATE, es posible incluir datos de copia de seguridad inactivos. La copia de seguridad incremental de los datos puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten.

Si está exportando a un medio secuencial: la clase de dispositivo que utilizan los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para exportar la información del nodo. El límite de montaje para la clase de dispositivo debe ser como mínimo 2.

Importante: Si se van a exportar los nodos cliente inscritos como TYPE=SERVER, debe especificar ALL, ARCHIVE o ALLACTIVE.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad *activas* e *inactivas*. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Este parámetro admite los valores siguientes:

ALL

El servidor exporta todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management.

None

El servidor no exporta archivos, sólo las definiciones de los nodos.

ARChive

El servidor sólo exporta las copias archivadas.

Backup

El servidor sólo exporta las versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

El servidor solo exporta las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato EXPORT.

ALLActive

El servidor exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato EXPORT.

SPacemanaged

El servidor exporta solo los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si se previsualiza el resultado de la operación de exportación, sin exportar la información. Puede utilizar este parámetro para previsualizar cuántos bytes de datos se transfieren de forma que pueda determinar cuántos volúmenes serán necesarios. Este parámetro admite los valores siguientes:

No

Especifica que se ha de exportar la información del nodo. Si especifica este valor, también debe especificar una clase de dispositivo.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades. Si especifica este valor, no es necesario especificar una clase de dispositivo.

Este parámetro es opcional. El valor predeterminado es NO.

DEVclass

Especifica la clase de dispositivo donde se han de grabar los datos de exportación. Este parámetro es necesario si especifica PREVIEW=NO.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la exportación, IBM Spectrum Protect cancela las operaciones con prioridad más baja para que haya una unidad disponible.

Consejo: Se pueden exportar los datos a una agrupación de almacenamiento de otro servidor especificando una clase de dispositivo que tenga el tipo de dispositivo SERVER.

Scratch

Especifica si se pueden utilizar volúmenes reutilizables. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que se pueden utilizar volúmenes reutilizables para la operación de exportación. Si especifica también una lista de volúmenes, los volúmenes reutilizables sólo se utilizan si no hay suficiente espacio en los volúmenes especificados.

No

Especifica que no pueden utilizarse volúmenes reutilizables para la exportación. Para determinar el número de volúmenes que puede necesitar, puede ejecutar el mandato especificando PREVIEW=YES.

VOLumenames

Especifica los volúmenes que se utilizarán para contener los datos exportados. Este parámetro es opcional, a no ser que especifique SCRATCH=NO y PREVIEW=NO. Si no especifica ningún nombre de volumen, se utilizan los volúmenes reutilizables.

Puede especificar uno de los siguientes valores:










nombre_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el mandato emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.

Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, pueden exportarse los datos de los que se ha hecho copia de seguridad después del parámetro TODATE o TOTIME. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia 10 días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00. Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro admite los valores siguientes:

No

Especifica que los datos no se exportarán desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que los datos pueden exportarse desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

Este parámetro es opcional. El valor predeterminado es NO.

Ejemplo: exportar información de nodo cliente a volúmenes de cinta específicos

Desde el servidor, exportar la información de nodo cliente a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1.

```
export node devclass=menu1 volumenames=tape01,tape02,tape03
```

Ejemplo: exportar información de nodo de cliente utilizando el FSID

Desde el servidor, utilice el FSID para exportar versiones de copias de seguridad activas de datos de archivos del nodo cliente JOE al volumen de cinta TAPE01. Para determinar el FSID, emita primero un mandato QUERY FILESPACE.

1. Para determinar el FSID, emita un mandato QUERY FILESPACE.

```
query file space joe
```

```
Node Name Filespace FSID Platform Filespace Is Capacity Pct
      archivos          forma          esp. (MB) Util.
      Unicode?
-----
```

JOE	\\joe\c\$	1	WinNT	NTFS	Sí	2.502,3 75,2
JOE	\\joe\d\$	2	WinNT	NTFS	Sí	6.173,4 59,6

- Exporte las versiones de copias de seguridad activas de los datos de archivos y especifique que el volumen de cinta debe ser utilizado por un dispositivo asignado a la clase de dispositivo MENU1.

```
export node joe fsid=1,2
filedata=backupactive devclass=menu1
volumenames=tape01
```

Ejemplo: exportar información de nodo cliente a los volúmenes de cinta que se indican en un archivo

Desde el servidor, exporte la información de nodo de cliente a cinta que figura en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA


El archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export node devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export node devclass=menu1 volumenames=file:tapevol.data
```

EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)

Utilice este mandato para exportar definiciones de nodos cliente o datos de archivos directamente a otro servidor para su importación inmediata.

Importante: No es posible exportar nodos de tipo NAS. El proceso de exportación excluirá estos nodos.

Puede suspender y reiniciar una operación de exportación de servidor a servidor que tenga un valor de FILEDATA distinto de NONE. El servidor guarda el estado de la operación de exportación para que se pueda reiniciar a partir del punto en que se encontraba cuando falló o se suspendió. La operación de exportación puede reiniciarse más adelante mediante la emisión del mandato RESTART EXPORT.

Importante: Una operación de exportación se suspende cuando se detecta una de estas condiciones:

- Se emite un mandato SUSPEND EXPORT para la operación de exportación que está en ejecución.
- Operación realizada por adelantado: otro proceso ha suprimido el archivo que se lee para la exportación.
- Errores de comunicaciones en una exportación de servidor a servidor.
- No hay puntos de montaje disponibles.
- Los volúmenes necesarios no están disponibles.
- Se han encontrado errores de E/S.

Emita el mandato QUERY EXPORT para que se visualice la información relacionada con las operaciones de exportación que están en ejecución y que se han suspendido.

La operación de exportación no se puede reiniciar si falla antes de transmitir al servidor de destino las definiciones de nodos y espacios de archivos seleccionables. Debe volver a especificar el mandato para empezar una nueva operación de exportación.

Puede emitir el mandato QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el mandato QUERY EXPORT para obtener una lista de todas las operaciones de exportación de servidor a servidor que pueden reiniciarse. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
.-*-----.  
>>-EXPort Node----->  
      '-nombre_nodo-'  
  
>----->  
      '-FILESpace---nombre_espacio_archivos-'  
  
>----->  
      '-FSID---identificador_espacio_archivos-'  
  
>----->  
      '-UNIFILESpace---nombre_espacio_archivos-'  
  
>----->  
      '-Domains---nombre_dominio-'  
  
.FILEData---None-----.  
>----->  
      '-FILEData---+All-----+'  
                +-None-----+  
                +-Archive-----+  
                +-Backup-----+  
                +-BACKUPActive-+  
                +-ALLActive----+  
                '-Spacemanged-'  
  
>----->  
      |                .FROMTime---00:00:00-. |  
      '-FROMDate---fecha-----+'  
                '-FROMTime---hora-----'  
  
>----->  
      |                .TOTime---23:59:59-. |  
      '-TODate---fecha-----+'  
                '-TOTime---hora-----'  
  
>----->  
      '-EXPORTIDentifier---identificador_exportación-'  
  
>----->  
      '-TOServer---nombre_servidor-'  
  
.PREVIEWImport---No-----.  
>----->  
      '-PREVIEWImport---+No--+-'  
                '-Yes-'  
  
.MERGEfilespace---No-----.  
>----->  
      '-MERGEfilespace---+No--+-'  
                '-Yes-'  
  
.Replacedefs---No-----.  
>----->  
      '-Replacedefs---+No--+-'  
                '-Yes-'  
  
.PROXynodeassoc---No-----.  
>----->  
      '-PROXynodeassoc---+No--+-'  
                '-Yes-'  
  
.ENCryptionstrength---AES-----.  
>----->  
      '-ENCryptionstrength---+AES--+-'  
                '-DES-'  
  
.ALLOWSHREDDable---No-----.  
>----->  
      '-ALLOWSHREDDable---+No--+-'  
                '-Yes-'
```

nombre_nodo

Especifica los nombres de nodos de cliente para los que se va a exportar la información. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Para cada nodo especificado, se realizará la búsqueda en todos los espacios de archivos del espacio de archivos, FSID, y en las listas habilitadas para Unicode.

Restricción: Si especifica una lista de nombres de nodo o patrones de nodo, el servidor no muestra los nombres o patrones de nodo que no coincidan con ninguna entrada de la base de datos. Compruebe las estadísticas de resumen de las anotaciones de actividades para verificar que el servidor haya exportado todos los nodos previstos.

FILESpace

Especifica los espacios de archivos para los que se van a exportar los datos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

Restricción: Si se especifica un espacio de archivos, no se exporta ningún espacio de archivos habilitado para Unicode.

FSID

Especifica los espacios de archivos utilizando sus identificadores de espacios de archivos (FSID). El servidor utiliza los identificadores FSID para encontrar los espacios de archivos que se deben exportar. Para buscar el FSID para un espacio de archivos, utilice el mandato QUERY FILESPACE. Puede separar varios identificadores de espacios de archivos con comas y sin espacios intercalados. Este parámetro es opcional.

UNIFILESpace

Especifica los espacios de archivos que el servidor reconoce como activados para Unicode. El servidor convierte los nombres entrados de la página de códigos del servidor a la página de códigos UTF-8 para encontrar los espacios de archivos a exportar. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizarse un carácter comodín para especificar un nombre. Este parámetro es opcional.

DOmains

Especifica los dominios de políticas desde donde se exportan los nodos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Si especifica dominios, IBM Spectrum Protect sólo exporta un nodo si pertenece a uno de los dominios especificados. Puede utilizar caracteres comodín para especificar un nombre.

FILEData

Especifica el tipo de archivos que se debe exportar para todos los nodos. Este parámetro es opcional. El valor predeterminado es NONE.

Nota: Si está exportando un nodo que tiene datos de grupo, los datos que no son parte de los objetos de destino podrían exportarse. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. Por ejemplo, si FILEDATA=BACKUPACTIVE cuando se especifican los parámetros FROMDATE o TODATE, es posible incluir datos de copia de seguridad inactivos. La copia de seguridad incremental de los datos puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten.

Si está exportando a un medio secuencial, la clase de dispositivo que utilizan los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo que se especifica en este mandato, IBM Spectrum Protect necesita dos unidades para exportar la información del nodo. El límite de montaje para la clase de dispositivo debe ser como mínimo 2.

Importante: Si exporta nodos cliente inscritos como TYPE=SERVER, especifique ALL, ARCHIVE o ALLACTIVE.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad *activas* e *inactivas*. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Los valores son los siguientes:

ALL

El servidor exporta todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management.

None

El servidor no exporta archivos, sólo las definiciones de los nodos.

ARchive

El servidor sólo exporta las copias archivadas.

Backup

El servidor sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

El servidor sólo exporta las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato EXPORT.

ALLActive

El servidor exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de

seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato EXPORT.

SPacemanaged

El servidor exporta solo los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.

Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, pueden exportarse los datos de los que se ha hecho copia de seguridad después del parámetro TODATE o TOTIME. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia 10 días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad de estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00. Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

TOTIME

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el mandato DEFINE SERVER. El administrador que emita el mandato de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

MERGEfilespace

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

PROXynodeassoc

Especifica si se exportan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no exporta datos desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que el servidor realiza la exportación desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

Restricción: Después de que una operación de exportación ha finalizado la identificación de los archivos que han de exportarse, los cambios que se realicen en el valor ALLOWSHREDABLE de la agrupación de almacenamiento se pasarán por alto. Una operación de exportación que se ha suspendido retiene el valor de ALLOWSHREDABLE original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor ALLOWSHREDABLE de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el mandato de exportación después de realizar la operación de limpieza necesaria.

EXPORTIdentifier

Este parámetro opcional especifica el nombre que ha seleccionado para identificar esta operación de exportación. Si no especifica un identificador, el servidor generará uno automáticamente. El nombre del identificador de exportación no puede tener más de 64 caracteres, no puede contener caracteres comodín y no es sensible a las mayúsculas y minúsculas. Puede utilizar el nombre del identificador para hacer referencia a las operaciones de exportación en los mandatos QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT o CANCEL EXPORT.

Restricción: debe especificar el parámetro TOSERVER si va a especificar el parámetro EXPORTIDENTIFIER. EXPORTIDENTIFIER se pasa por alto si FILEDATA=NONE.

Ejemplo: exportar información de nodo cliente y todos los archivos de cliente

Para exportar información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB, emita el mandato siguiente:

```
export node nodel filedata=all toserver=serverb
```

Ejemplo: exportar información de nodo cliente y todos los archivos de un rango de fechas específico

Para exportar información de nodo cliente y todos los archivos para NODE1 directamente a SERVERB entre el 1 de febrero de 2009 y la fecha de hoy.

```
export node nodel filedata=all toserver=serverb  
fromdate=02/01/2009 todate=today
```

Ejemplo: exportar información de nodo cliente y todos los archivos de cliente de un rango de fechas y horas específico

Para exportar la información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB entre las 8:00 horas del 1 de febrero de 2009 y las 08:00 de hoy, emita el mandato siguiente:

```
export node nodel filedata=all toserver=serverb  
fromdate=02/01/2009  
fromtime=08:00:00  
todate=today totime=08:00:00
```

Ejemplo: exportar información de nodo cliente y todos los archivos de cliente de los tres últimos días

Para exportar la información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB de los tres últimos días, emita el mandato siguiente:

```
export node nodel filedata=all toserver=serverb  
fromdate=today -3
```

EXPORT POLICY (Exportar información de políticas)

Utilice este mandato para exportar la información de la política desde un servidor de IBM Spectrum Protect a un medio secuencial o directamente a otro servidor para su importación inmediata. Cuando se exporta una política utilizando el mandato EXPORT POLICY, la información de la agrupación de datos activos del dominio no se exporta.

El servidor exporta información de políticas, como por ejemplo:

- Definiciones del dominio de políticas
- Definiciones del juego de políticas, incluido el juego de políticas activo
- Definiciones de la clase de gestión, incluida la clase de gestión predeterminada
- Definiciones de grupo de copia de seguridad y de grupo de copia archivada
- Definiciones de planificación de cada dominio de políticas
- Asociaciones de nodos cliente, si el nodo cliente existe en el servidor destino

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de exportación. También puede ver esta información desde la consola del servidor.










Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si exporta información de políticas a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el mandato emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

Ejemplo: exportar información de política a volúmenes de cinta específicos

Desde el servidor, exportar la información de políticas a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
export policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Ejemplo: exportar información de política a los volúmenes de cinta que se indican en un archivo




Desde el servidor, exporte la información de política a volúmenes de cinta que figuren en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA

Este archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato siguiente:

```
 Sistemas operativos AIX  Sistemas operativos Linux
export policy devclass=menu1 volumenames=file:tapevol
 Sistemas operativos Windows
export policy devclass=menu1 volumenames=file:tapevol.data
```

EXPORT POLICY (Exportar una política directamente a otro servidor)

Utilice este mandato para exportar información de políticas directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

Para supervisar el progreso de la operación de importación, puede emitir un mandato QUERY PROCESS desde el servidor de destino. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Utilice este mandato para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente (si está especificado) del servidor a un medio secuencial.

Si exporta información del servidor a un medio secuencial, luego puede utilizar el medio para importar la información a otro servidor con un tipo de dispositivo compatible.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

También tiene la opción de procesar una operación de exportación directamente a otro servidor de la red. Esto da como resultado un proceso de importación inmediato sin que sean necesarios tipos de dispositivos secuenciales compatibles entre los dos servidores.

Puede exportar los siguientes tipos de información del servidor emitiendo el mandato EXPORT SERVER:

- Definiciones del dominio de políticas
- Definiciones del juego de políticas
- Definiciones de clase de gestión y grupo de copia
- Planificaciones definidas para cada dominio de políticas
- Definiciones de administrador
- Definiciones de los nodos cliente

De forma opcional, puede exportar los siguientes tipos de datos:

- Definiciones de espacio de archivos
- Información de autorización de acceso relativa a los espacios de archivos exportados
- Copias de seguridad, copias archivadas y archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si exporta información del servidor a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados estará incompleto y no deberá utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación.

Emita el mandato QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el mandato QUERY EXPORT para obtener una lista de todas las operaciones de exportación de servidor a servidor (que tienen un valor FILEDATA distinto de NONE) que están en ejecución o que se han suspendido.

Puede utilizar el mandato QUERY ACTLOG para ver la información de estado real que indica el tamaño y si la operación de exportación ha sido satisfactoria o no.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.
- Los mandatos EXPORT NODE y EXPORT SERVER no exportan datos de una agrupación de fragmentación a menos que lo permita de forma explícita estableciendo el parámetro ALLOWSHREDDABLE en el valor YES. Si se especifica este valor y los datos exportados incluyen datos de agrupaciones de destrucción, esos datos no se podrán destruir. No se emite ningún aviso si la operación de exportación incluye datos de agrupaciones de fragmentación.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
 - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.
 - Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
 - Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESPPACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

El mandato EXPORT SERVER ofrece dos posibilidades: exportación directa a otro servidor de la red o bien exportación a un medio secuencial. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con EXPORT SERVER

Mandato	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

- EXPORT SERVER (Exportar un servidor a medios secuenciales)
Puede exportar toda la información de control del servidor o parte de ella y los datos de archivos de cliente de un servidor a un medio secuencial, de modo que esta información se puede importar a otro servidor.
- EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)
Utilice este mandato para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

EXPORT SERVER (Exportar un servidor a medios secuenciales)

Puede exportar toda la información de control del servidor o parte de ella y los datos de archivos de cliente de un servidor a un medio secuencial, de modo que esta información se puede importar a otro servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.-FILEData---None-----
>>-EXPort Server-----+----->
    '-FILEData---+All-----+'
                        +-None-----+
                        +-ARchive-----+
                        +-Backup-----+
                        +-BACKUPActive-+
                        +-ALLActive----+
                        '-SPacemanaged-'

.-Preview ---No-----
>+-----+----->
|          (1) (2)          |
'-Preview-----+No--+-'
                        '-Yes-'

>+-----+----->
|          (1)          |
'-DEVclass-----nombre_clase_dispositivo-'

.-Scratch---Yes-----
>+-----+----->
|          (2)          |
'-Scratch-----+Yes--+-'
                        '-No--'

>+-----+----->
|          (2)          |          |
|          V          |          |
'-VOLumenames-----+---nombre_volumen+---+-'
                        '-FILE:--nombre_archivo-'

>+-----+----->
'-USEDVolumelist---nombre_archivo-'

>+-----+----->
|          .-FROMTime---00:00:00- |
'-FROMDate---fecha-----+-----+'
                        '-FROMTime---hora-----'

>+-----+----->
|          .-TOTime---23:59:59- |
'-TODate---fecha-----+-----+'
                        '-TOTime---hora-----'

.-ENCryptionstrength---AES-----
>+-----+----->
'-ENCryptionstrength---+AES--+-'
                        '-DES-'

.-ALLOWSHREDDable---No-----
>+-----+----->
'-ALLOWSHREDDable---+No--+-'
                        '-Yes-'

```

Notas:

1. Si PREVIEW=NO, debe especificarse una clase de dispositivo.
2. Si PREVIEW=NO y SCRATCH=NO, debe especificarse uno o más volúmenes.

Parámetros

FILEData

Especifica el tipo de archivo que se exportan para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Si está exportando a un medio secuencial, la clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para exportar la información del servidor. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad *activas* e *inactivas*. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Los valores siguientes están disponibles:

ALL

IBM Spectrum Protect exporta todas las versiones de copia de seguridad de archivos, todas las copias archivadas y todos los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no exporta archivos, sólo las definiciones.

ARchive

IBM Spectrum Protect sólo exporta las copias archivadas.

Backup

IBM Spectrum Protect sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo exporta las versiones de copia de seguridad activas.

ALLActive

IBM Spectrum Protect exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se migraron mediante el cliente IBM Spectrum Protect for Space Management.

SPacemanaged

IBM Spectrum Protect exporta solo los archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si desea previsualizar el resultado de la operación de exportación, sin exportar la información. Puede utilizar este parámetro para obtener la previsualización del número de bytes de datos que se transferirán y, por lo tanto, podrá determinar cuántos volúmenes serán necesarios. Este parámetro admite los valores siguientes:

No

Especifica que se ha de exportar la información del servidor. Si especifica este valor, también debe especificar una clase de dispositivo.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades. Si especifica este valor, no es necesario especificar una clase de dispositivo.

Este parámetro es opcional. El valor predeterminado es NO.

DEVclass

Especifica la clase de dispositivo donde se han de grabar los datos de exportación. Este parámetro es necesario si especifica PREVIEW=NO.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la exportación, IBM Spectrum Protect cancela las operaciones con prioridad más baja para que haya una unidad disponible.

Consejo: Se pueden exportar los datos a una agrupación de almacenamiento de otro servidor especificando una clase de dispositivo que tenga el tipo de dispositivo SERVER.

Scratch

Especifica si se pueden utilizar volúmenes reutilizables. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que se pueden utilizar volúmenes reutilizables para la operación de exportación. Si especifica también una lista de volúmenes, los volúmenes reutilizables sólo se utilizan si no hay suficiente espacio en los volúmenes especificados.

No

Especifica que no pueden utilizarse volúmenes reutilizables para la exportación. Para determinar el número de volúmenes que puede necesitar, puede ejecutar el mandato especificando PREVIEW=YES.

VOLumenames

Especifica los volúmenes que se utilizarán para contener los datos exportados. Este parámetro es opcional, a no ser que especifique SCRATCH=NO y PREVIEW=NO. Si no especifica ningún nombre de volumen, se utilizan los volúmenes reutilizables.

Puede especificar uno de los siguientes valores:










nombre_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el mandato emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.
Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.
Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según

lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME+=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00. Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que los datos no se exportarán desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que los datos pueden exportarse desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

Ejemplo: exportar un servidor a volúmenes de cinta específicos

Desde el servidor, exportar la información del servidor a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
export server devclass=menu1
volumenames=tape01,tape02,tape03
```

Ejemplo: exportar un servidor desde los volúmenes de cinta que se indican en un archivo

Desde el servidor, exporte la información de servidor a volúmenes de cinta que figuren en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA


El archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export server devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export server devclass=menu1 volumenames=file:tapevol.data
```

EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)

Utilice este mandato para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

Las operaciones de exportación de servidor a servidor que tienen un valor para FILEDATA distinto de NONE se pueden reiniciar después de haberlas suspendido. El servidor guarda el estado de la operación de exportación para que se pueda reiniciar a partir del punto en que se encontraba cuando falló o se suspendió. La operación de exportación puede reiniciarse posteriormente mediante la emisión del mandato RESTART EXPORT. Estas operaciones de exportación se pueden suspender y reiniciar manualmente. Por consiguiente, si se produce un error en una exportación, ésta se suspende automáticamente si ha completado la fase de definiciones de transmisión.

Una operación de exportación se suspende cuando se detecta una de estas condiciones:

- Se emite un mandato SUSPEND EXPORT para la operación de exportación que está en ejecución.
- Operación realizada por adelantado: otro proceso ha suprimido el archivo que se va a leer para la exportación.
- Errores de comunicaciones en una exportación de servidor a servidor.
- No hay puntos de montaje disponibles.
- Los volúmenes necesarios no están disponibles.
- Se han encontrado errores de E/S.

La operación de exportación no se puede reiniciar si falla antes de transmitir al servidor de destino las definiciones de nodos y espacios de archivos seleccionables. Debe volver a especificar el mandato para empezar una nueva operación de exportación.

Emita el mandato QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el mandato QUERY EXPORT para obtener una lista de todas las operaciones de exportación de servidor a servidor (que tienen un valor FILEDATA distinto de NONE) que están en ejecución o que se han suspendido. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.-FILEData---None-----
>>-EXPort Server-----+----->
    '-FILEData---+All-----+'
                    +-None-----+
                    +-ARChive-----+
                    +-Backup-----+
                    +-BACKUPActive-+
                    +-ALLActive----+
                    '-SPacemanaged-'

>+-----+-----+----->
|                               .-FROMTime---00:00:00-. |
'-FROMDate---fecha-----+'
                    '-FROMTime---hora-----'

>+-----+-----+----->
|                               .-TOTime---23:59:59-. |
'-TODate---fecha-----+'
                    '-TOTime---hora-----'

>+-----+-----+----->
'-EXPORTIDentifier---identificador_exportación-'

>+-----+-----+----->
'-TOServer---nombre_servidor-'

.-PREVIEWImport---No-----
>+-----+-----+----->
'-PREVIEWImport---+No--+-'
                    '-Yes-'

.-MERGEfilespace---No-----
>+-----+-----+----->
'-MERGEfilespace---+No--+-'
                    '-Yes-'

.-Replacedefs---No-----
>+-----+-----+----->
'-Replacedefs---+No--+-'
                    '-Yes-'

.-PROXynodeassoc---No-----
>+-----+-----+----->
'-PROXynodeassoc---+No--+-'
                    '-Yes-'

.-ENCryptionstrength---AES-----
>+-----+-----+----->
'-ENCryptionstrength---+AES--+-'
                    '-DES-'

.-ALLOWSHREDDable---No-----
>+-----+-----+----->
'-ALLOWSHREDDable---+No--+-'
                    '-Yes-'

```

Parámetros

FILEData

Especifica el tipo de los archivos que deben exportarse para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Si está exportando a un medio secuencial: la clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, IBM Spectrum Protect necesita dos unidades para exportar la información del servidor. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad activas e inactivas. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Los valores son:

ALL

IBM Spectrum Protect exporta todas las versiones de copia de seguridad de archivos, todas las copias archivadas y todos los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no exporta archivos, sólo las definiciones.

ARchive

IBM Spectrum Protect sólo exporta las copias archivadas.

Backup

IBM Spectrum Protect sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo exporta las versiones de copia de seguridad activas.

ALLActive

IBM Spectrum Protect exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se migraron mediante el cliente IBM Spectrum Protect for Space Management.

SPacemanaged

IBM Spectrum Protect exporta solo los archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.

Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el

03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08

Valor	Descripción	Ejemplo
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00. Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00. Si ejecuta este mandato a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el mandato DEFINE SERVER. El administrador que emita el mandato de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

MERGEfilespace

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

PROXynodeassoc

Especifica si se exportan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no admite la exportación de datos desde una agrupación que aplica la destrucción.

Yes

Especifica que el servidor admite la exportación de datos desde una agrupación que aplica la destrucción. Los datos del medio de exportación no se destruirán.

Importante: Después de que una operación de exportación ha finalizado la identificación de los archivos que han de exportarse, los cambios que se realicen en el valor ALLOWSHREDABLE de la agrupación de almacenamiento se pasarán por alto. Una operación de exportación que se ha suspendido retiene el valor de ALLOWSHREDABLE original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor ALLOWSHREDABLE de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el mandato de exportación después de realizar la operación de limpieza necesaria.

EXPORTIdentifier

Este parámetro opcional especifica el nombre que ha seleccionado para identificar esta operación de exportación. Si no especifica un nombre de mandato, el servidor generará uno automáticamente. El nombre del identificador de exportación no puede tener más de 64 caracteres, no puede contener caracteres comodín y no es sensible a las mayúsculas y minúsculas. Puede utilizar el nombre del identificador para hacer referencia a las operaciones de exportación en los mandatos QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT o CANCEL EXPORT. EXPORTIDENTIFIER se pasa por alto si FILEDATA=NONE o si PREVIEWIMPORT=YES.

Si especifica el parámetro EXPORTIDENTIFIER, debe especificar el parámetro TOSERVER.

Ejemplo: exportar información de servidor directamente a otro servidor

Para exportar información de servidor directamente a SERVERB, emita el mandato siguiente.

```
export server filedata=all toserver=serverb
```

Ejemplo: exportar información de servidor directamente a otro servidor utilizando un rango de fechas

Para exportar directamente a SERVERB entre el 1 de febrero de 2009 y la fecha actual, emita el mandato siguiente.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

Ejemplo: exportar información de servidor y datos de archivo de cliente directamente a otro servidor utilizando un rango de fechas y de horas

Para exportar directamente a SERVERB desde las 8:00 horas del 1 de febrero de 2009 hasta la fecha actual, a las 8:00 horas, emita el mandato siguiente.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

EXTEND DBSPACE (Incrementar el espacio para la base de datos)

Utilice este mandato para aumentar el espacio para la base de datos añadiendo directorios para que los utilice la base de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Cuando se emite el mandato EXTEND DBSPACE, los directorios se añaden a la base de datos. Con los valores de parámetro predeterminados, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama espacio de almacenamiento. Esta acción mejora el rendimiento de E/S paralela y hace que el espacio de nuevo directorio esté disponible para su uso inmediato.

Si no desea redistribuir los datos al añadir nuevos directorios, puede especificar RECLAIMSTORAGE=NO. Si especifica NO para este parámetro, se llenará todo el espacio en los directorios existentes antes de utilizar los nuevos directorios. Puede redistribuir los datos y solicitar espacio más adelante, pero debe completar el procedimiento manual que requiere esta tarea utilizando mandatos de DB2.

Restricción: La redistribución de datos y la reclamación de espacio como parte de una operación para ampliar el espacio de base de datos solo funciona con espacios de tabla de DB2 versión 9.7 o posterior. Los espacios de tablas se crean al formatear un nuevo servidor IBM Spectrum Protect Versión 6.2 o posterior. Si actualizó o restauró el servidor de IBM Spectrum Protect desde V6.1, no puede redistribuir datos ni reclamar espacio. Debe emitir el mandato EXTEND DBSPACE con RECLAIMSTORAGE=NO.

Importante: El proceso de redistribución utiliza un número considerable de recursos del sistema, por lo tanto, asegúrese de planificarlo con antelación cuando desee añadir espacio a la base de datos. Revise las indicaciones siguientes:

- Complete el proceso cuando el servidor no esté gestionando mucha carga de trabajo.
- El tiempo que se necesita para redistribuir datos y reclamar espacio puede variar. Se ve afectado por factores tales como el diseño del sistema de archivos, la proporción de rutas nuevas a rutas de almacenamiento existentes y operaciones simultáneas. Para obtener una estimación aproximada, puede intentar la operación con una pequeña base de datos de IBM Spectrum Protect en un sistema de laboratorio. Utilice los resultados como referencia para estimar el tiempo necesario para el procedimiento.
- No interrumpa el proceso de redistribución. Si intenta detener, por ejemplo, el proceso que está completando el trabajo, debe detener y reiniciar el servidor de DB2. Cuando se reinicia el servidor, éste se colocará en la modalidad de recuperación del accidente, la cual tarda varios minutos, y después se reanuda el proceso de redistribución.

Después de que se haya completado una operación para ampliar el espacio de base de datos, detenga y reinicie el servidor para poder utilizar completamente los directorios nuevos. Si los directorios de bases de datos existentes están casi llenos cuando se añade un nuevo directorio, el servidor puede recibir una condición de falta de espacio (que se notifica en db2diag.log). Puede corregir la condición de falta de espacio deteniendo y reiniciando el servidor.

Sintaxis


```
      .-|-----|
      v         |
>>-EXTend DBSpace---directorio_bd+----->

.-REclaimstorage---Yes-----.-Wait---No-----
>>+-----+-----+-----+-----<<
' -REclaimstorage---+No---' ' -Wait---+No---'
```

Parámetros

directorio_bd (Necesario)

Especifica los directorios para el almacenamiento de la base de datos. Los directorios deben estar vacíos y ser accesibles con el ID de usuario del gestor de bases de datos. Un nombre de directorio debe ser un nombre totalmente calificado y no puede superar los 175 caracteres de longitud. Especifique el nombre entre comillas si éste contiene espacios en blanco intercalados, un signo igual u otros caracteres especiales. Si está especificando una lista de directorios para el almacenamiento de datos, la longitud máxima de la lista puede ser de 1400 caracteres.

 Sistemas operativos Windows Restricción: No se pueden especificar rutas UNC (convenio universal de nomenclatura).

Consejo: Especifique directorios con el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

REClaimstorage

Especifica si los datos se redistribuyen entre los directorios de base de datos recién creados y si se reclama espacio desde las vías de acceso de almacenamiento antiguas. Este parámetro es opcional. El valor predeterminado es Yes (sí).

A menos que especifique `WAIT=YES`, la operación se ha completado como un proceso en segundo plano.

Yes

Especifica que los datos se redistribuyen de modo que los directorios nuevos quedan disponibles para su uso inmediato. Importante: El proceso de redistribución utiliza un número considerable de recursos del sistema, por lo que debe asegurarse de planificarlo con antelación.

Una vez que el proceso se inicia, se emiten mensajes que le informarán acerca del progreso. Puede utilizar el mandato `QUERY PROCESS` para supervisar la operación. Para cancelar el proceso, puede utilizar el mandato `CANCEL PROCESS`, pero si una operación de redistribución de datos está en curso, se completará antes de que el proceso se haya detenido.

No

Especifica que los datos no se redistribuyen entre los directorios de base de datos y no se reclama espacio de almacenamiento cuando se añade espacio para la base de datos.

Wait



Especifica si el mandato se procesa de forma subordinada o en primer plano.

No

Especifica el proceso subordinado. El valor predeterminado es NO.

Yes

Especifica el proceso en primer plano.

 Sistemas operativos AIX  Sistemas operativos Linux No se puede especificar YES desde la consola del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: agregar directorios al espacio de almacenamiento para la base de datos, redistribuir datos y solicitar espacio.

Añadir dos directorios (/tsm_db/stg1 y /tsm_db/stg2) debajo del directorio /tsm_db al espacio de almacenamiento para la base de datos. Emita el mandato:

```
extend dbspace /tsm_db/stg1,/tsm_db/stg2
```

 Sistemas operativos Windows

Ejemplo: agregar controladores al espacio de almacenamiento para la base de datos, redistribuir datos y solicitar espacio.

Agregar las unidades D y E al espacio de almacenamiento para la base de datos. Emita el mandato:

```
extend dbspace D:,E:
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con EXTEND DBSPACE




Mandato	Descripción
DSMSERV EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

Tareas relacionadas:

Gestión de la capacidad de inventario

Mandatos GENERATE

Utilice los mandatos GENERATE para los conjuntos de copia de seguridad para un espacio de archivos o un nodo cliente seleccionado.

- GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)
- GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)

GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)

Utilice este mandato para generar un juego de copias de seguridad para un nodo de cliente de archivado y copia de seguridad. Un *juego de copias de seguridad* es una recopilación de los datos activos con copia de seguridad de un cliente de archivado y copia de seguridad, almacenados y gestionados como un solo objeto, en medios específicos, en el almacenamiento del servidor. Aunque puede crear un juego de copias de seguridad para cualquier nodo de cliente, sólo puede utilizarlo un cliente de archivado y copia de seguridad.

Restricción: Un juego de copias de seguridad con el "formato de eliminación de duplicados" tiene esta designación como resultado de un mandato GENERATE BACKUPSET con al menos una de las especificaciones siguientes:

- Incluye un nodo en el cliente de archivado y copia de seguridad Versión 6.1.x (como mínimo 6.1.0 pero inferior a V6.2.0).
- Incluye un nodo que tiene uno o más nodos autorizados para actuar como un proxy. Como mínimo uno de estos nodos proxy está en el cliente de archivado y copia de seguridad V6.1.x.

Los conjuntos de copias de seguridad en el formato de eliminación de duplicados sólo se pueden restaurar mediante el cliente de archivado y copia de seguridad V6.1.2 o posterior. Los clientes de archivado y copia de seguridad anteriores a V6.1.2 no se pueden restaurar del conjunto de copias de seguridad en el formato de eliminación de duplicados.

Un juego de copias de seguridad con el "formato de eliminación de duplicados distribuido" tiene esta designación como resultado de un mandato GENERATE BACKUPSET con al menos una de las especificaciones siguientes:

- Incluye un nodo en el nivel de cliente de archivado y copia de seguridad V6.2.0 o posterior.
- Incluye un nodo que tiene uno o más nodos autorizados para actuar como un proxy. Como mínimo uno de estos nodos proxy está en el cliente de archivado y copia de seguridad V6.2.0.

Los conjuntos de copias de seguridad con el formato de eliminación de duplicados distribuido sólo se pueden restaurar mediante el cliente de archivado y copia de seguridad V6.2.0 o posterior.

Restricción: No puede generar un juego de copias de seguridad con archivos de los que se haya realizado copia de seguridad en IBM Spectrum Protect utilizando NDMP. Sin embargo, puede crear un juego de copias de seguridad con archivos de los que se ha realizado copia de seguridad utilizando la diferencia de instantánea NetApp.

El servidor crea las copias de las versiones activas de los objetos con copia de seguridad de un cliente que están dentro de uno o más espacios de archivos con este mandato. A continuación, el servidor las consolida en medios secuenciales. Actualmente, los tipos de objeto de copia de seguridad que están admitidos para los juegos de copias de seguridad sólo incluyen directorios y archivos.

El nodo de cliente de archivado y copia de seguridad puede restaurar el juego de copias de seguridad desde el servidor y desde el medio en el que se ha grabado el juego de copias de seguridad.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela el proceso subordinado que ha creado este mandato, es posible que el medio no contenga un juego de copias de seguridad completo. Puede utilizar el mandato QUERY PROCESS para mostrar información acerca del proceso subordinado que crea este mandato.

Consejo: Cuando IBM Spectrum Protect genera un juego de copias de seguridad, puede mejorar el rendimiento si las agrupaciones de almacenamiento primarias que contienen los datos de cliente están próximas. Si está próxima una agrupación de almacenamiento

primaria, es muy probable que los datos del nodo cliente ocupen menos volúmenes de cinta que los que ocuparían si la agrupación de almacenamiento no estuviera próxima. Con la proximidad, se emplea menos tiempo en buscar entradas de base de datos, y se necesitan menos operaciones de montaje.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

Sintaxis

```

      .-,------.
      V           |
>>-GENerate BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'

>--prefijo_nombre_juego_copias_seguridad----->

      .-*------.
>+-----+-----+-----+-----+----->
      | .-,------. |
      | V           | |
      |'---nombre_espacio_archivos-+-'

>--DEVclass-----nombre_clase_dispositivo----->

      .-SCRatch-----Yes-----.
>+-----+-----+-----+-----+----->
      '-SCRatch-----+Yes-+-'
      '-No--'

>+-----+-----+-----+-----+----->
      | .-,------. |
      | V           | |
      |'-VOLumes-----nombres_volúmenes-+-'

      .-RETention-----365-----.
>+-----+-----+-----+-----+----->
      '-RETention-----+días-+-'
      '-NOLimit-'

      .-Wait-----No-----.
>+-----+-----+-----+-----+----->
      '-DESCription-----descripción-' '-Wait-----+No-+-'
      '-Yes-'

      .-NAMEType-----SERVER-----.
>+-----+-----+-----+-----+----->
      '-NAMEType-----+SERVER-+-'
      '+UNiCode+'
      '-FSID----'

      .-CODEType-----BOTH------.
>+-----+-----+-----+-----+----->
      '-CODEType-----+UNiCode-+-'
      '+NONUNiCode+'
      '-BOTH-----'

      .-PITDate-----current_date-. .-PITTime-----current_time-.
>+-----+-----+-----+-----+----->
      '-PITDate-----date-----' '-PITTime-----time-----'

      .-DATAType-----FILE------. .-TOC-----Preferred-----.
>+-----+-----+-----+-----+----->
      | .-,------. | '-TOC-----+No-----+-'
      | V           | | '+Preferred+'
      |'-DATAType-----+FILE-+-' '-Yes-----'
      '+IMAGE+'
      '-ALL----'

>+-----+-----+-----+-----+----->
      '-TOCMGmtclass-----nombre_clase-'

      .-ALLOWSHREDdable-----No-----.
>+-----+-----+-----+-----+-----><

```

'-ALLOWSHREDDable--=---+No---+'
'-Yes-'

Parámetros

nombre_nodo o nombre_grupo_nodos (Necesario)

Especifica el nombre del nodo cliente y grupos de nodos cuyos datos se incluyen en el juego de copias de seguridad. Para especificar varios nombres de nodo y nombres de grupos de nodos, sepárelos con comas y sin espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos. Cuando se especifican varios nombres de nodo, el servidor genera un juego de copias de seguridad para cada nodo y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida.

prefijo_nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad del nodo cliente. La longitud máxima del nombre es de 30 caracteres.

Cuando selecciona un nombre, IBM Spectrum Protect agrega un sufijo para crear el nombre de juego de copias de seguridad. Por ejemplo, si especifica el nombre del juego de copias de seguridad *mybackupset*, IBM Spectrum Protect agrega un número exclusivo como, por ejemplo, 3099, al nombre. El nombre de juego de copias de seguridad se identifica en IBM Spectrum Protect como *mybackupset.3099*. Para mostrar posteriormente información acerca de este juego de copias de seguridad, puede incluir un comodín en el nombre, como *mybackupset.** o puede especificar el nombre calificado al completo, como *mybackupset.3099*.

Cuando se especifican varios nombres de nodo, el servidor genera un juego de copias de seguridad para cada nodo y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida. A cada juego de copias de seguridad se otorga el mismo nombre completo que consta del *prefijo_nombre_juegos_copias_seguridad* y un sufijo determinado por el servidor.

nombre_espacio_archivos

Especifica el nombre de uno o varios espacios de archivos que contienen los datos que se van a incluir en el juego de copias de seguridad. Este parámetro es opcional. El nombre de espacio de archivos que se especifique puede contener caracteres comodín. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Si no especifica un espacio de archivos, en el juego de copias de seguridad se incluirán todos los espacios de archivos activos de los que se ha realizado copia de seguridad de los nodos de cliente.

Para un servidor que tenga clientes con soporte para espacios de archivos habilitados para Unicode, puede especificar un nombre de espacio de archivos o bien un ID de espacio de archivos (FSID). Si especifica un nombre de espacio de archivos, puede que el servidor tenga que convertir el nombre del espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para conocer los detalles. Si no especifica ningún nombre de espacio de archivos o especifica sólo un carácter comodín para dicho nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo de los volúmenes donde se grabará el juego de copias de seguridad. La longitud máxima del nombre es de 30 caracteres.

Restricción: No es posible especificar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA .

SCRatch

Especifica si se utilizarán volúmenes reutilizables para el juego de copias de seguridad. Si incluye una lista de volúmenes mediante el parámetro VOLUMES, el servidor sólo utiliza los volúmenes reutilizables si los volúmenes especificados no pueden contener los datos. El valor predeterminado es SCRATCH=YES. Los valores son:

YES

Especifica que se utilizarán volúmenes reutilizables para el juego de copias de seguridad.

NO

Especifica que no se utilizarán volúmenes reutilizables para el juego de copias de seguridad.

VOLumes

Especifica el nombre de uno o varios volúmenes que contendrán el juego de copias de seguridad. Este parámetro es opcional. Puede especificar más de un volumen separando cada volumen con una coma y sin espacios intercalados.

Si no especifica este parámetro, se utilizan los volúmenes reutilizables para el juego de copias de seguridad.

RETention

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor. Puede especificar un entero entre el 0 y el 30000. El valor predeterminado es 365 días. Los valores son:

días

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor.

NOLimit

Especifica que el juego de copias de seguridad debe retenerse indefinidamente en el servidor.

Si especifica NOLIMIT, el servidor retendrá los volúmenes que contienen el juego de copias de seguridad sin límite de tiempo, a menos que un usuario o un administrador suprima los volúmenes del almacenamiento del servidor.

DEScRiption

Especifica la descripción que se asociará al juego de copias de seguridad. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores son:

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes que se crean no se visualizan hasta que el mandato haya finalizado el proceso. No se puede especificar WAIT=YES desde la consola del servidor.

No

Especifica que el mandato se procesa de forma subordinada. Utilice el mandato QUERY PROCESS para supervisar el proceso subordinado de este mandato.

NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten espacios de archivos activados para Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que utilizan sistemas operativos Windows, NetWare o Macintosh OS X.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID). Importante: Preste atención al especificar este parámetro si también se han especificado varios nombres de nodo. Es posible que nodos diferentes utilicen el mismo ID de espacio de archivos para diferentes espacios de archivos, o diferentes ID de espacio de archivos para el mismo nombre de espacio de archivos. Por esta razón, especificar un ID de espacio de archivos como los nombres de espacio de archivos podría hacer que para algunos nodos se graben los datos incorrectos en el juego de copias de seguridad.

CODEType

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre del espacio de archivos o cuando no especifique ningún nombre de espacio de archivos. Los valores posibles son:

UNICODE

Incluir sólo los espacios de archivos que están en Unicode.

NONUNICODE

Incluir sólo los espacios de archivos que no están en Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

PITDate

Especifica que los archivos que estaban activos en la fecha especificada y que aún se almacenan en el servidor de IBM Spectrum Protect deben incluirse en el juego de copias de seguridad, aunque estén inactivos en el momento de emitir el mandato. Este parámetro es opcional. El valor predeterminado es la fecha en la que se ejecuta el mandato GENERATE BACKUPSET. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7. Para incluir archivos que estaban activos hace una semana, especifique PITDATE=TODAY-7 o PITDATE=-7
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

PITTime

Especifica que los archivos que estaban activos a la hora especificada y que aún se almacenan en el servidor de IBM Spectrum Protect deben incluirse en el juego de copias de seguridad, aunque estén inactivos en el momento de emitir el mandato. Este parámetro es opcional. Si se ha especificado una fecha PITDate, el valor predeterminado es medianoche (00:00:00); en caso contrario, el valor predeterminado es la hora a la que se ha iniciado el mandato GENERATE BACKUPSET. Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha PIT especificada	12:33:28
NOW	La fecha actual en la fecha PIT especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha PIT especificada	NOW+03:00 o +03:00 Si emite este mandato a las 9:00 con PITTIME=NOW+03:00 o PITTIME=+03:00. IBM Spectrum Protect incluirá archivos que estaban activos a las 12:00 en la fecha PIT.

DATATYPE

Especifica que se van a generar los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que se deben generar juegos de copias de seguridad de nivel de archivo. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados.

El servidor genera un juego de copias de seguridad para cada tipo de datos y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida. A cada juego de copias de seguridad se otorga el mismo nombre completo que consta del *prefijo_nombre_juegos_copias_seguridad* y un sufijo determinado por el servidor. Sin embargo, cada juego de copias de seguridad tiene un tipo de datos diferente, tal como muestra el mandato QUERY BACKUPSET. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) de los que se ha hecho una copia de seguridad en el servidor se deben generar.

FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a generar. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad. Si el cliente de copia de seguridad no ha realizado copia de seguridad de ningún archivo o directorio, no se generará un juego de copias de seguridad de nivel de archivo. Este es el valor predeterminado.

IMAGE

Especifica que se va a generar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad. Los juegos de copias de seguridad de imagen se generan sólo si un cliente de copia de seguridad ha realizado copia de seguridad de una imagen.

TOC

Especifica si debe guardarse una tabla de contenido (TOC) para cada juego de copias de seguridad de nivel de archivo. Las tablas de contenido siempre se guardan para conjuntos de copias de seguridad que contienen datos de imagen o aplicación. Se ignorará el parámetro TOC al generar juegos de copias de seguridad de imagen y aplicación. Siempre se generará una tabla de contenido para los juegos de copias de seguridad de imagen y aplicación.

Cuando determine si desea guardar una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se guarda una tabla de contenido para un juego de copias de seguridad, podrá utilizar el cliente web de copia de seguridad/archivado de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse. Para crear una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión que especifica el parámetro TOCMGMTCLASS. Para la creación de una tabla de contenido se necesitan de forma adicional procesos, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación del juego de copias de seguridad.
- Si no se guarda una tabla de contenido para un juego de copias de seguridad, todavía podrá restaurar archivos individuales o árboles de directorios mediante el mandato RESTORE BACKUPSET del cliente de copia de seguridad/archivado, siempre que conozca el nombre cualificado completo de cada archivo o directorio que se desea restaurar.

Para que se visualice el contenido de los juegos de copias de seguridad, también puede utilizar el mandato QUERY BACKUPSETCONTENTS.

Este parámetro es opcional. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para los juegos de copias de seguridad de nivel de archivo.

Preferred

Especifica que la información de la tabla de contenido deberá guardarse para los juegos de copias de seguridad de nivel de archivo. Este es el valor predeterminado. Sin embargo, un juego de copias de seguridad no fallará sólo porque se produzca un error durante la creación de la tabla de contenido.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada juego de copias de seguridad de nivel de archivo. Un juego de copias de seguridad fallará si se produce un error durante la creación de la tabla de contenido.

TOCMgmtclass

Especifica el nombre de la clase de gestión a la que debe estar vinculada la tabla de contenido. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado el nodo. En este caso, la creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que implementa la destrucción de datos se incluyen en el juego de copias de seguridad. Este parámetro es opcional. Los valores posibles son:

No

Especifica que los datos de una agrupación de almacenamiento que implementa la destrucción de datos no se incluyen en el juego de copias de seguridad. Este es el valor predeterminado.

Yes

Especifica que los datos de una agrupación de almacenamiento que implementa la destrucción de datos pueden incluirse en el juego de copias de seguridad. Los datos del medio del juego de copias de seguridad no se destruirán.

Ejemplo: generar un juego de copias de seguridad de un espacio de archivos

Generar un juego de copias de seguridad de un espacio de archivos denominado /srvr que pertenece al nodo de cliente JANE. Denominar el juego de copias de seguridad PERS_DATA y retenerlo durante 75 días. Especifique que los volúmenes VOL1 y VOL2 contienen los datos del juego de copias de seguridad. Los volúmenes los ha de leer un dispositivo asignado a la clase de dispositivo AGADM. Incluya una descripción.

```
generate backupset jane pers_data /srvr devclass=agadm
retention=75 volumes=vol1,vol2
description="area 51 base image"
```

Ejemplo: generar un juego de copias de seguridad de un espacio de archivos habilitado para Unicode

Generar un juego de copias de seguridad de un espacio de archivos habilitado para Unicode, \\joe\c\$, que pertenece al nodo cliente JOE. Dé al conjunto de copia de seguridad el nombre JOES_DATA. Especificar que el volumen VOL1 contiene los datos del conjunto de

copia de seguridad. El volumen debe ser leído por un dispositivo asignado a la clase de dispositivo AGADM. Utilice el servidor para que éste convierta el nombre del espacio de archivos \\joe\c\$ de la página de códigos del servidor en la página de códigos UTF-8.

```
generate backupset joe joes_data \\joe\c$ devclass=agadm
volumes=vol1 nametype=unicode
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con GENERATE BACKUPSET

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)

Utilice este mandato para generar una tabla de contenido para un juego de copias de seguridad que todavía no disponga de una. El cliente de copia de seguridad/archivado utiliza la tabla de contenido para visualizar el juego de copias de seguridad, lo cual permite a los usuarios seleccionar los archivos individuales que desea restaurar del mismo.

La creación de una tabla de contenido para un juego de copias de seguridad necesita espacio de agrupación de almacenamiento y, posiblemente, uno o más puntos de montaje durante la operación de creación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

Sintaxis

```
>>-GENerate BACKUPSETTOC--nombre_nodo--nombre_juego_copias_seguridad-->
  .-DATAType-----ALL-----
>----->
|           .-,-----|
|           v         |
|'-DATAType-----+FILE-----'
```

'-IMAGE-'

>+-----+-----<<
'-TOCMGmtclass-----nombre_clase-'

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente cuyos datos están contenidos en el juego de copias de seguridad. No se pueden utilizar caracteres comodín para especificar un nombre ni se puede especificar una lista de nombres de nodos cliente.

nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad del nodo cliente. No se pueden utilizar caracteres comodín para especificar un nombre ni se puede especificar una lista de nombres de juegos de copias de seguridad.

DATATYPE

Especifica el tipo de datos que se va a incluir en la tabla de contenido. Este parámetro es opcional. De manera predeterminada se incluyen todos los datos. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que la tabla de contenido incluye todos los tipos de datos (nivel de archivo, imagen y aplicación) almacenados en el juego de copias de seguridad. Este es el valor predeterminado.

FILE

Especifica que la tabla de contenido sólo incluye los datos de nivel de archivo. Los datos de nivel de archivo comprenden los archivos y directorios de los que se ha hecho copia de seguridad mediante el cliente de copia de seguridad/archivado. Si el juego de copias de seguridad no contiene ningún archivo ni directorio, no se generará la tabla de contenido.

IMAGE

Especifica que la tabla de contenido incluirá únicamente las copias de seguridad de imágenes. Las copias de seguridad de imágenes comprenden las imágenes del sistema de archivos creadas mediante el mandato BACKUP IMAGE del cliente de copias de seguridad. Si el juego de copias de seguridad no contiene ninguna copia de seguridad de imagen, no se generará la tabla de contenido.

TOCMGmtclass

Especifica el nombre de la clase de gestión a la que debe estar vinculada la tabla de contenido. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado el nodo. Si crea una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

Ejemplo: generar una tabla de contenido

Genere una tabla de contenido para un juego de copias de seguridad denominado PROJX_DATA que contiene los datos para el nodo cliente GARY. La tabla de contenido se encontrará en la clase de gestión predeterminada.




```
generate backupsettoc gary projx_data
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con GENERATE BACKUPSETTOC

Mandato	Descripción
COPY ACTIVE DATA	Copia los datos de copia de seguridad activos.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.

Mandato	Descripción
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)

Utilice este mandato para generar estadísticas de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o una agrupación de almacenamiento de contenedores en la nube, a fin de determinar el rendimiento de la deduplicación de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento.

Sintaxis

```
>>-GENerate DEDUPStats--nombre_agrupación----->
      .-,-----
      | v |
>-----+---nombre_nodo-----+----->
      | '-nombre_grupo_nodos-'
      .-*-----
>-----+----->
      | .-,-----
      | | v | |
      +---nombre_espacio_de_archivos---+
      | .-,-----
      | | v | |
      |'-----FSID-----'
      .-CODEType----BOTH----- .-MAXProcess----4-----
>-----+-----+----->
      | '-CODEType----+UNICODE----' | '-MAXProcess----numero-'
      | +NONUNICODE+
      | '-BOTH-----'
      .-NAMEType----SERVER----- .-Wait----No-----
>-----+-----+-----><
      | '-NAMEType----+SERVER---+' | '-Wait----+No---+'
      | +UNICODE+
      | '-FSID----'
      | '-Yes-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se notifica en las estadísticas de eliminación de duplicados de datos. Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el mandato falla.

Restricción: Puede especificar únicamente agrupaciones de almacenamiento de contenedores de directorios o agrupaciones de almacenamiento en la nube.

nombre_nodo o nombre_grupo_nodos (Necesario)

Especifica el nombre del nodo de cliente o el grupo definido de nodos de cliente que se notifican en las estadísticas de deduplicación de datos. También puede especificar una combinación de nombres de nodos de cliente y nombres de grupos de nodos de cliente. Para especificar varios nombres de nodos de cliente o nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede utilizar caracteres comodín con los nombres de nodos de cliente pero no con los nombres de grupos de nodos de cliente.

nombre_espacio_de_archivos o FSID

Especifica el nombre de uno o varios espacios de archivos en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. El asterisco es el valor predeterminado. Especifique uno de los siguientes valores:

*

Especifique un asterisco (*) para mostrar todos los espacios de archivos o ID.

nombre_espacio_de_archivos

Especifica el nombre del espacio de archivos. Especifique varios nombres separándolos con comas y sin espacios intercalados. FSID especifica un identificador de espacio de archivo. Este parámetro es válido para los clientes con espacios de archivos que están en formato Unicode. Especifique varios nombres separándolos con comas y sin espacios intercalados.

Para los clientes con espacios de archivos en formato Unicode, puede especificar un nombre de espacio de archivos o un FSID. Si especifica un nombre de espacio de archivos, es posible que el servidor deba convertir el nombre de espacio de archivos que especifique. Por ejemplo, puede que el servidor deba convertir el nombre que especifique de la página de códigos del servidor a Unicode.

Restricciones: Se aplican las restricciones siguientes a los nombres de espacio de archivos y FSID:

- Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.
- No especifique FSID y nombres de espacio de archivos en el mismo mandato.

CODEType

Especifica qué tipo de espacios de archivos se van a incluir en el registro. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un asterisco para visualizar información sobre todos los espacios de archivos. Este parámetro es opcional. Especifique uno de los siguientes valores:

UNICODE

Incluir los espacios de archivos que están en formato Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en formato Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos. Este es el valor predeterminado.

MAXProcess

Especifica el número máximo de procesos paralelos que se utilizarán para generar estadísticas para un contenedor en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro cuando los clientes de IBM Spectrum Protect tengan espacios de archivos en formato Unicode y estén en sistemas operativos Windows, NetWare o Macintosh OS X. Este parámetro es opcional.

Este parámetro es necesario si especifica un nombre de nodo y un nombre de espacio de archivos o un FSID.

Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un asterisco.

Especifique uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor.

Consejo: La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivo como sus FSID.

Wait

Especifica si las estadísticas de deduplicación de datos se generan en primer o en segundo plano. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras se está procesando el mandato. Los mensajes relacionados con el proceso en segundo plano se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Éste es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe finalizar para poder continuar con otras tareas. Los mensajes se muestran en el archivo de registro de actividades o la consola de servidor, o en ambos, en función de la ubicación en la que se registren los mensajes.

Restricción: No puede especificar el parámetro WAIT=YES desde la consola de servidor.

Ejemplo: generar estadísticas de eliminación de duplicados de datos para un espacio de archivos

Generar estadísticas de deduplicación de datos para un espacio de archivos llamado /srvr que pertenece a una agrupación de almacenamiento de contenedores de directorio, POOL1, que está almacenada en el nodo de cliente NODE1.

```
generate dedupstats pool1 node1 /srvr
```







Ejemplo: generar estadísticas de deduplicación de datos para un espacio de archivos habilitado para Unicode

Genere las estadísticas de deduplicación de datos para un espacio de archivos habilitado para Unicode denominado \\abc\c\$ que pertenece al nodo de cliente NODE2. Convierta el nombre de espacio de archivo \\abc\c\$ de la página de códigos del servidor a la página de códigos UTF-8.

```
generate dedupstats node2 \\abc\c$ nametype=unicode
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con GENERATE DEDUPSTATS

Mandato	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDELETE DEDUPSTATS	Suprime las estadísticas de eliminación de duplicados de datos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsQUERY DEDUPSTATS	Muestra las estadísticas de eliminación de duplicados de datos.

Mandatos GRANT

Utilice el mandato GRANT para otorgar el acceso o los privilegios apropiados.

- GRANT AUTHORITY (agregar autorización de administrador)
- GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)

GRANT AUTHORITY (agregar autorización de administrador)

Utilice este mandato para otorgar a un administrador una o varias clases de privilegios de administración y autorización para acceder a nodos cliente.

No puede otorgar privilegios restringidos a un administrador con privilegio de almacenamiento sin restricciones o de política sin restricciones. Debe utilizar el mandato REVOKE AUTHORITY para eliminar el privilegio sin restricciones del administrador; a continuación, utilice este mandato para otorgar privilegios restringidos al administrador.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-GRant AUTHority--nombre_admin----->
      .-,------.
      (1)  V          |
>--Classes-----+SYstem-----+----->
      +-Policy-----+
      +-STorage-----+
      +-Operator-----+
      '-Node--| A |-'

>+-----+-----+----->
|          .-,------. |
|          V          | |
| '-DOmains-----nombre_dominio-+-'

>+-----+-----+-----<
|          .-,------. |
|          (1)  V          | |
| '-STGpools-----nombre_agrupación-+-'

A

.-AUTHority---Access-----
|+-----+-----+----->
| '-AUTHority---+Access-+-'
|         '-Owner--'

>--+DOmains-----nombre_dominio+-----|
| '-Node-----node_name-----'

```

Notas:

1. Debe especificar uno o más de estos parámetros.

Parámetros

nombre_admin (Necesario)

Especifica el nombre del administrador al que se le otorgará la clase de privilegio de administración.

Classes

Especifica una o varias clases de privilegio que se otorgan a un administrador. Este parámetro es necesario, excepto cuando se especifica el parámetro STGPOOLS. Puede especificar más de una clase de privilegio separando cada una con una coma. Las clases posibles son:

System

Especifica que desea otorgar privilegios del sistema a un administrador. Un administrador del sistema tiene el nivel de autorización más alto de IBM Spectrum Protect. Un administrador del sistema puede emitir cualquier mandato de administración y tiene autorización para gestionar todos los dominios de políticas y todas las agrupaciones de almacenamiento. No especifique clases de privilegio adicionales ni los parámetros DOMAINS o STGPOOLS cuando otorgue privilegio de sistema a un administrador. Únicamente un administrador del sistema puede otorgar autorización a otros administradores.

Policy

Especifica que desea otorgar privilegios de políticas a un administrador. Si no especifica el parámetro DOMAINS, se otorga el privilegio de políticas sin restricciones. Un administrador con privilegio de política sin restricciones puede emitir mandatos que afecten a todos los dominios de políticas existentes, al igual que a cualquier dominio de políticas que se defina posteriormente. Un administrador con privilegio de políticas sin restricciones no puede definir, suprimir o copiar dominios de políticas. Utilice el mandato GRANT AUTHORITY con CLASSES=POLICY y sin ningún parámetro DOMAINS para convertir a un administrador de políticas restringidas en un administrador de políticas sin restricciones.

STorage

Especifica que desea otorgar privilegios de almacenamiento a un administrador. Si no se especifica el parámetro STGPOOLS, se otorga un privilegio de almacenamiento sin restricciones. Un administrador con privilegio de almacenamiento sin restricciones puede emitir todos los mandatos que asignen y controlen recursos de almacenamiento del servidor. Un administrador con privilegio de almacenamiento sin restricciones puede emitir mandatos que afecten a todas las agrupaciones de almacenamiento existentes, al igual que a cualquier agrupación de almacenamiento que se defina posteriormente. Un administrador con privilegio de almacenamiento sin restricciones no puede definir ni suprimir agrupaciones de almacenamiento. Si se utiliza el mandato GRANT AUTHORITY con CLASSES=STORAGE y ningún parámetro STGPOOLS, un administrador con almacenamiento restringido se puede convertir en un administrador con almacenamiento sin restricciones.

Operator

Especifica que desea otorgar privilegios de operador a un administrador. Un administrador con privilegio de operador puede emitir mandatos que controlan la operación inmediata del servidor y la disponibilidad del medio de almacenamiento.

Node

Especifica que desea otorgar privilegios de nodo a un administrador. Un usuario con privilegio de nodo cliente puede acceder remotamente a un cliente de copia de seguridad/archivado de Web con un identificador de usuario y contraseña de administración, si tiene autorización de propietario o autorización de acceso. La autorización de acceso es el valor predeterminado para la clase de privilegio de nodo.

Atención: Al especificar la clase de privilegio de nodo, también debe especificar el parámetro DOMAIN o el parámetro NODE, pero no los dos.

AUTHORITY

Especifica el nivel de autorización de un usuario con privilegio de nodo. Este parámetro es opcional.

Si un administrador ya tiene privilegio de sistema o de políticas para el dominio de políticas al que pertenece el nodo, este mandato no modificará el privilegio del administrador.

Los niveles de autorización posibles son:

Access

Especifica que desea otorgar autorización de acceso a cliente a un usuario con la clase de privilegio de nodo. Es el valor predeterminado si se ha especificado CLASSES=NODE. Un usuario con autorización de acceso a cliente puede acceder a un cliente de copia de seguridad/archivado de Web y ejecutar acciones de copia de seguridad y restauración para ese cliente.

Atención: Un usuario con autorización de acceso a cliente no puede acceder a ese cliente desde otro sistema utilizando el parámetro -VIRTUALNODENAME.

Un nodo cliente puede establecer la opción REVOKEREMOTEACCESS para restringir el acceso de un usuario que tiene privilegio de nodo con autorización de acceso a cliente a una estación de trabajo cliente que está ejecutando un cliente de Web. Esta opción no afecta a los administradores con autorización de propietario de cliente, privilegio de sistema o privilegio de políticas para el dominio de políticas al que pertenece el nodo.

Owner

Especifica que desea otorgar autorización de propietario de cliente a un usuario con la clase de privilegio de nodo. Un usuario con autorización de propietario de cliente puede acceder a un cliente de copia de seguridad/archivado de Web mediante la interfaz de cliente de Web y también acceder a los datos desde otro cliente utilizando el parámetro -VIRTUALNODENAME.

DOmains

Especifica que desea otorgar al administrador autorización de acceso a cliente o de propietario de cliente para todos los clientes del dominio de políticas especificado. Este parámetro no se puede utilizar junto con el parámetro NODE.

NODE

Especifica que desea otorgar al administrador autorización de acceso a cliente o de propietario de cliente para el nodo. Este parámetro no se puede utilizar junto con el parámetro DOMAIN.

DOmains

Cuando se utiliza con CLASSES=POLICY, especifica que desea otorgar a un administrador el privilegio de política con restricciones.

El privilegio de políticas con restricciones permite a un administrador emitir un subconjunto de mandatos de políticas para los dominios sobre los que el administrador tiene autorización. Puede utilizar este parámetro para otorgar autorización de dominio de políticas a un administrador de políticas con restricciones. Este parámetro es opcional. Puede especificar más de un dominio de políticas delimitando cada uno con una coma.

Puede utilizar caracteres comodín para especificar un nombre. Se otorgará autorización para todos los dominios de políticas coincidentes.

STGpools

Especifica que desea otorgar a un administrador privilegios de almacenamiento con restricciones. Si se especifica el parámetro STGPools, entonces CLASSES=STORAGE es opcional.

El privilegio de almacenamiento con restricciones permite emitir un subconjunto de mandatos de almacenamiento para las agrupaciones de almacenamiento sobre las que el administrador tiene autorización. Puede utilizar este parámetro para otorgar autorización de agrupación de almacenamiento a un administrador de almacenamiento con restricciones. Este parámetro es opcional. Puede especificar más de una agrupación de almacenamiento delimitando cada una con una coma.

Puede utilizar caracteres comodín para especificar un nombre. Se otorgará autorización para todas las agrupaciones de almacenamiento que coincidan.

Ejemplo: otorgar privilegio de sistema a un administrador

Otorgar privilegio de sistema al administrador Larry.

```
grant authority larry classes=system
```

Ejemplo: otorgar acceso a dominios de políticas adicionales

Especificar dominios de políticas adicionales que pueda gestionar el administrador CLAUDIA con privilegio de políticas restringido.

```
grant authority claudia domains=employee_records,progl
```

Ejemplo: proporcionar a un administrador privilegio de almacenamiento sin restricciones y privilegio de políticas restringido

Proporcionar al administrador TOM privilegio de almacenamiento sin restricciones y privilegio de políticas sin restricciones para los dominios cuyos nombres comiencen por EMP.

```
grant authority tom classes=storage  
domains=emp*
```

Ejemplo: otorgar a un administrador autorización restringida a un nodo específico

Otorgar privilegio de nodo al usuario HELP para que el personal del departamento de soporte pueda ayudar al nodo de cliente LABCLIENT a hacer copia de seguridad o a restaurar datos sin tener otros privilegios de IBM Spectrum Protect de nivel superior.

```
grant authority help classes=node node=labclient
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con GRANT AUTHORITY

Mandato	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
REVOKE AUTHORITY	Revoca una o más clases de privilegio o limita el acceso a los dominios de políticas y agrupaciones de almacenamiento.

GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)

Utilice este mandato para otorgar una autoridad proxy a un nodo cliente del servidor de IBM Spectrum Protect.

Los nodos cliente de destino poseen los datos y los nodos agente actúan en nombre de los nodos de destino. Cuando se otorga autorización de proxy a un nodo cliente de destino, un nodo agente puede realizar operaciones de copia de seguridad y de restauración para el nodo de destino. Los datos que almacena el nodo agente en nombre del nodo de destino se almacena bajo el nombre del nodo de destino en el almacenamiento del servidor.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones

Sintaxis

```
>>-GRant PROXynode TArget--===nombre_nodo_destino----->  
>--AGent--===nombre_nodo_agente-----<
```

Parámetros

Target (Obligatorio)

Especifica el nombre del nodo propietario de los datos. No se pueden utilizar nombres comodín para especificar el nombre de nodo de destino.

AGent (Obligatorio)

Especifica el nombre del nodo que realiza operaciones para el nodo de destino. El nodo agente no tiene que estar en el mismo dominio que el nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.

Ejemplo: otorgar autorización de proxy a un nodo cliente

Imaginemos que MOE y JOE son nodos agente de un clúster NAS y que éstos se utilizan para realizar la copia de seguridad y restauración de datos NAS compartidos. Para crear una relación de autorización de proxy para el nodo de destino NASCLUSTER, emita el mandato siguiente:

```
grant proxynode target=nascluster agent=moe,joe
```

Emita el siguiente mandato en el nodo de destino MOE para realizar la copia de seguridad de los datos del clúster NAS que se almacenan en la unidad E:. El nombre del nodo de destino es NASCLUSTER.

```
dsmc -asnode=nascluster incremental e:
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con GRANT PROXYNODE

Mandato	Descripción
QUERY PROXYNODE	Visualiza los nodos con autoridad para actuar como nodos proxy.
REVOKE PROXYNODE	Revocar la autoridad de proxy a un nodo de agente.

HALT (Concluir el servidor)

Utilice este mandato para concluir el servidor. El mandato HALT fuerza una conclusión precipitada, que cancela todas las sesiones de nodo cliente y de administración, aunque no se hayan completado.

Cualquier transacción en proceso que haya interrumpido el mandato HALT se retrotraerá cuando vuelva a arrancar el servidor. Utilice el mandato HALT sólo después de que se hayan completado o cancelado las sesiones de nodo cliente y de administración. Para concluir el servidor sin que las sesiones de nodo cliente o de administración sufran un impacto grave, realice los pasos siguientes:

1. Utilice el mandato DISABLE SESSIONS para impedir que se inicien nuevas sesiones de nodo cliente.
2. Utilice el mandato QUERY SESSIONS para identificar las sesiones de nodo cliente y de administración existentes.
3. Notifique a cualquier sesión de nodo cliente o de administración que piensa concluir el servidor (debe realizarlo fuera de IBM Spectrum Protect).
4. Utilice el mandato CANCEL SESSIONS para cancelar las sesiones de nodo cliente o de administración existentes.
5. Emita el mandato HALT para concluir el servidor y detener las sesiones de nodo cliente y de administración existentes.

Consejo:

La acción del mandato HALT puede obtenerse con la opción de servidor ALIASHALT. Utilice la opción del servidor para definir un término distinto de HALT que realice la misma función. El mandato HALT conserva su función normal; sin embargo, la opción del servidor proporciona un método adicional para emitir el mandato HALT. Consulte el apartado ALIASHALT para obtener más información.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de operador.

Sintaxis

```
>>-HALT-----<<
```

Parámetros

Ninguno.

Ejemplo: concluir el servidor

Concluir el servidor, desde la consola del servidor o desde un cliente de administración. Toda la actividad de usuario se parará inmediatamente y no se podrá iniciar ninguna nueva actividad.

```
halt
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con HALT

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.

HELP (Obtener ayuda sobre mandatos y mensajes de error)

Utilice este mandato para visualizar los mandatos de administración y los mensajes de error. Puede emitir el mandato desde un cliente de línea de mandatos de administración.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Help-----<<
+-número_tema_ayuda-----+
|           .-,----- . |
|           v             |
+-nombre_mandato-----+
|           '-nombre_submandato-' |
+-número_mensaje-----+
+-nombre_opción_servidor-----+
+'-nombre_programa_utilidad-----'
```

Parámetros

número_tema_ayuda

Especifica el número de su selección de los temas de ayuda. Este parámetro es opcional.

Los números de tema se muestran en la tabla de contenidos, por ejemplo:

```
3.0 Administrative commands
...
3.13.10 DEFINE DEVCLASS (Definir una clase de dispositivo)
  3.13.10.1 DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
  3.13.10.2 DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
  ...
```

El número de tema para el mandato DEFINE DEVCLASS para una clase de dispositivo 3592 es 3.13.10.2.

nombre_mandato

Especifica el nombre del mandato de administración que desea visualizar. Este parámetro es opcional.

nombre_submandato

Especifica un máximo de dos nombres de submandato asociados al nombre del mandato de administración que desea visualizar. Este parámetro es opcional.

número_mensaje

Especifica el número del mensaje para el que desea visualizar información. Este parámetro es opcional. Puede obtener información de ayuda sobre mensajes del servidor (con el prefijo ANR) y mensajes del cliente (con el prefijo ANE o ANS). No incluya el prefijo ni el código de gravedad cuando especifique un número de mensaje de error.

nombre_opción_servidor

Especifica el nombre de un servidor sobre el que desea visualizar información. Este parámetro es opcional.

nombre_programa_utilidad

Especifica el nombre del programa de utilidad de servidor sobre el que desea visualizar información. Este parámetro es opcional.

Ejemplo: visualizar los temas de la ayuda

Visualizar los temas de ayuda para la interfaz de la línea de mandatos.

```
ayuda
```

Salida parcial:

```
1.0 Administración del servidor desde la línea de mandatos
  1.1 Emisión de mandatos desde el cliente de administración
    1.1.1 Inicio y detención del cliente de administración
    1.1.2 Supervisión de actividades del servidor desde el cliente de
        administración
```

Ejemplo: visualizar un tema de la ayuda con el número del tema de la ayuda

Visualizar información de ayuda con el número del tema de la ayuda. El número de tema para el mandato DEFINE DEVCLASS para una clase de dispositivo 3592 es 3.13.10.2.

```
help 3.13.10.2
```

Ejemplo: visualizar ayuda para un mandato

Visualizar información de ayuda acerca de los mandatos REMOVE.

```
help remove
```

```
Mandatos 3.44 REMOVE
Utilice los mandatos REMOVE para eliminar un objeto.
A continuación se muestra una lista de los mandatos REMOVE:
* 3.44.1, "REMOVE ADMIN (Eliminar un administrador)"
* 3.44.2, "REMOVE NODE (Eliminar un nodo o un nodo asociado
    a una máquina)"
```

Ejemplo: visualizar ayuda para un mensaje de error específico

Visualizar información de ayuda sobre el mensaje de error ANR2535E.

```
help 2535
```

```
Mandato
ANR2535E: no es posible eliminar el nombre del nodo ni cambiarle el nombre
porque tiene un transportador de datos
asociado.
Explicación: ha intentado eliminar o cambiar el nombre de un nodo
que tiene un
transportador de datos asociado.
Acción del sistema: el servidor no elimina ni cambia el nombre
del nodo.
Respuesta del usuario: para eliminar o cambiar el nombre del nodo,
elimine el transportador de datos
asociado y vuelva a emitir
el mandato.
```

Ejemplo: visualizar ayuda para una opción específica

Visualizar la descripción, la sintaxis y un ejemplo de la opción de servidor COMMMETHOD.

Ejemplo: visualizar ayuda para un programa de utilidad específico

Visualizar la descripción, la sintaxis y un ejemplo del programa de utilidad DSMSErv.

```
help dsmserv
```

IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)

Utilice este mandato para iniciar o detener procesos que identifiquen datos duplicados en una agrupación de almacenamiento. Puede especificar el número de proceso de identificación de duplicados y su duración.

Cuando cree una nueva agrupación de almacenamiento para la eliminación de datos duplicados, puede especificar entre 0 y 50 procesos de identificación de duplicados. IBM Spectrum Protect inicia el número especificado de procesos de identificación de duplicados automáticamente, cuando se inicia el servidor. Si no los detiene, éstos se ejecutarán indefinidamente.

Este mandato solo afecta al proceso de eliminación de duplicados del lado del servidor. En el proceso de eliminación de datos duplicados del lado del cliente, los duplicados se identifican en el cliente de copia de seguridad y archivado.

Con el mandato IDENTIFY DUPLICATES puede iniciar procesos adicionales, detener algunos o todos los procesos y especificar la cantidad de tiempo que el cambio ha de permanecer en vigor. Si ha aumentado o disminuido el número de procesos de identificación de duplicados, puede utilizar el mandato IDENTIFY DUPLICATES para restablecer el número de procesos en el número especificado en la definición de agrupación de almacenamiento.

Si no ha especificado ningún proceso de identificación de duplicados en la definición de la agrupación de almacenamiento, puede utilizar el mandato IDENTIFY DUPLICATES para iniciar y detener todos los procesos manualmente.

Este mandato inicia y detiene un proceso o procesos subordinados que puede cancelar con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Importante:

- También puede cambiar el número de procesos de identificación de duplicados mediante la actualización de la definición de agrupación de almacenamiento ejecutando el mandato UPDATE STGPOOL. No obstante, cuando actualice una definición de agrupación de almacenamiento, no puede especificar una duración. Los procesos que especifica en la definición de agrupación de almacenamiento se ejecutan indefinidamente, o hasta que emite el mandato IDENTIFY DUPLICATES, vuelve a actualizar la definición de agrupación de almacenamiento o cancela un proceso.

La emisión de IDENTIFY DUPLICATES no cambia el valor del número de procesos de identificación de duplicados en la definición de la agrupación de almacenamiento.

- Los procesos de identificación de duplicados pueden estar activos o inactivos. Los procesos que eliminan los duplicados de archivos están activos. Los procesos que esperan a que se eliminen los archivos duplicados están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. Los procesos sólo finalizan cuando se cancelan o cuando se cambia el número de procesos de identificación de duplicados para la agrupación de almacenado a un valor inferior al valor especificado. Antes de que se detenga un proceso de identificación de duplicados, éste debe finalizar el archivo cuyos duplicados está eliminando.

La salida del mandato QUERY PROCESS para un proceso de identificación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de identificación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es nueve.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-IDentify DUPLICates--nombre_agrupación_almacenamiento----->
>--+-----+-----+-----+-----><
```

Parámetros

nombre_agrupación_almacenamiento (Necesario)

Especifica el nombre de la agrupación de almacenamiento en la que han de identificarse los datos de duplicados. Puede utilizar comodines.

NUMProcess

Especifica el número de proceso de identificación de duplicados que deben ejecutarse después de que termine de ejecutarse el mandato. Puede especificar entre 0 y 50 procesos. El valor que especifique para este parámetro alterará temporalmente el valor que se ha especificado en la definición de la agrupación de almacenamiento o el valor más reciente que se ha especificado al emitir este mandato por última vez. Si especifica cero, todos los procesos de identificación de duplicados finalizarán.

Este parámetro es opcional. Si no especifica ningún valor, el servidor iniciará o detendrá los procesos de identificación de duplicados para que el número de procesos sea igual al número especificado en la definición de la agrupación de almacenamiento.

Por ejemplo, imaginemos que define una nueva agrupación de almacenamiento y que especifica dos procesos de identificación de duplicados. Posteriormente, emite el mandato IDENTIFY DUPLICATES para incrementar el número de procesos a cuatro. Cuando vuelva a emitir el mandato IDENTIFY DUPLICATES sin especificar ningún valor para el parámetro NUMPROCESS, el servidor detendrá dos procesos de identificación de duplicados.

Si ha especificado cero procesos al definir la agrupación de almacenamiento y emite IDENTIFY DUPLICATES sin especificar un valor para NUMPROCESS, todos los procesos de identificación de duplicados que están en ejecución se detendrán y el servidor no empezará ningún proceso nuevo.

Recuerde: Si especifica IDENTIFY DUPLICATES sin indicar un valor para NUMPROCESS, el parámetro DURATION no estará disponible. Los procesos de identificación de duplicados especificados en la definición de agrupación de almacenamiento se ejecutan indefinidamente, o hasta que vuelve a emitir el mandato IDENTIFY DUPLICATES, actualiza la definición de la agrupación de almacenamiento o cancela un proceso.

Cuando el servidor detiene un proceso de identificación de duplicados, el proceso completa el archivo físico actual y, a continuación, finaliza. Como consecuencia, puede tardar varios minutos en alcanzar el número de procesos de identificación de duplicados que especificó como valor para este parámetro.

DURation

Especifica el número máximo de minutos (1 - 9999) que este mandato deberá permanecer en vigor. Al final del tiempo especificado, el servidor iniciará o finalizará los procesos de identificación de duplicados para que el número de procesos sea el mismo que el número especificado en la definición de la agrupación de almacenamiento.

Este parámetro es opcional. Si no especifica un valor, los procesos que se ejecutan después de emitir el mandato, lo harán indefinidamente. Sólo finalizarán si vuelve a emitir el mandato IDENTIFY DUPLICATES, actualiza la definición de la agrupación de almacenamiento o cancela un proceso.

Por ejemplo, si define una agrupación de almacenamiento con dos procesos de identificación de duplicados y emite el mandato IDENTIFY DUPLICATES con `DURATION=60` y `NUMPROCESS=4`, el servidor iniciará dos procesos de identificación de duplicados adicionales que se ejecutarán durante sesenta minutos. Una vez transcurrido este tiempo, dos procesos finalizarán los archivos en los que están trabajando y se detendrán. Los dos procesos que se detienen podrían no ser los dos mismos procesos que se han iniciado como resultado de la emisión de este mandato.

El servidor finalizará primero los procesos inactivos. Si, después de finalizar todos los procesos inactivos, es preciso finalizar más procesos, el servidor lo notificará a los procesos activos que deben finalizar.

Cuando el servidor detiene un proceso de identificación de duplicados, el proceso completa el archivo físico actual y, a continuación, finaliza. Como consecuencia, puede tardar varios minutos en llegar a la cantidad de tiempo especificada como valor para este parámetro.

Ejemplo: controlar el número y la duración de los procesos de identificación de duplicados

En este ejemplo, ha especificado tres procesos de identificación de duplicados en la definición de la agrupación de almacenamiento. El mandato IDENTIFY DUPLICATES se usa para cambiar el número de procesos y especificar la cantidad de tiempo que permanecerá en vigor el cambio.

Tabla 1. Control manual de los procesos de identificación de duplicados

La definición de la agrupación de almacenamiento especifica tres procesos de identificación de duplicados. Con el mandato IDENTIFY DUPLICATES, especifica...	...y una duración de...	El resultado es...
2 procesos de identificación de duplicados	No se especifica	Un proceso de identificación de duplicados finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. Dos procesos se ejecutan indefinidamente, o hasta que vuelva a emitir el mandato IDENTIFY DUPLICATES, actualice la definición de la agrupación de almacenamiento o cancele un proceso.
	60 minutos	Un proceso de identificación de duplicados finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. Transcurridos 60 minutos, el servidor inicia un proceso para que existan tres procesos en ejecución.
4 procesos de identificación de duplicados	No se especifica	El servidor inicia un proceso de identificación de duplicados. Cuatro procesos se ejecutan indefinidamente, o hasta que vuelva a emitir el mandato IDENTIFY DUPLICATES, actualice la definición de la agrupación de almacenamiento o cancele un proceso.
	60 minutos	El servidor inicia un proceso de identificación de duplicados. Transcurridos los 60 minutos, un proceso finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. El proceso adicional que ha iniciado este mandato podría no ser uno de los que han de detenerse cuando haya transcurrido la duración indicada.
0 procesos de identificación de duplicados	No se especifica	Todos los procesos de identificación de duplicados finalizan los archivos en los que están trabajando, si los hay, y se detienen. Este cambio dura indefinidamente o hasta que pueda volver a emitir el mandato IDENTIFY DUPLICATES, actualizar la definición de la agrupación de almacenamiento o cancelar un proceso.
	60 minutos	Todos los procesos de identificación de duplicados finalizan los archivos en los que están trabajando, si los hay, y se detienen. Transcurridos los sesenta minutos, el servidor inicia tres procesos.
No se especifica	No disponible	El número de procesos de identificación de duplicados se restablece en el número de procesos especificado en la definición de la agrupación de almacenamiento. Este cambio dura indefinidamente o hasta que pueda volver a emitir el mandato IDENTIFY DUPLICATES, actualizar la definición de la agrupación de almacenamiento o cancelar un proceso.

Ejemplo: identificar duplicados en una agrupación de almacenamiento

Identifique duplicados en una agrupación de almacenamiento, STGPOOLA, utilizando tres procesos de identificación de duplicados. Especificar que este cambio permanezca en vigor durante 60 minutos.

```
identify duplicates stgpoola duration=60 numprocess=3
```

Mandatos relacionados

Tabla 2. Mandatos relacionados con IDENTIFY DUPLICATES

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.

Mandato	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

Mandatos IMPORT

Utilice los mandatos IMPORT para importar información desde los medios de exportación a un servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

- IMPORT ADMIN (Importar información del administrador)
- IMPORT NODE (Importar información de nodos clientes)
- IMPORT POLICY (Importar información de políticas)
- IMPORT SERVER (Importar información del servidor)

IMPORT ADMIN (Importar información del administrador)

Utilice este mandato para importar definiciones de administrador y de autorización para uno o varios administradores del medio de exportación al servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de importación.

También puede ver esta información desde la consola del servidor.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela el proceso subordinado IMPORT ADMIN, ya están importados algunos datos. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Restricción:

- Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
- Si la definición del administrador que se importa incluye autorización de analista, se importa la definición del administrador pero no así la autorización de analista. La autorización de analista no es válida para servidores con la versión 6.1 o superior.
- No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-Import Admin-----+----->
      | .-,-----+----->
      | V         | |
      |---nombre_admin---+--->

.-Preview ----No-----+----->
>---+-----+----->
  '-Preview-----+No---+-'
      '-Yes-'

>--DEVclass-----nombre_clase_dispositivo-----+----->

      .-,-----+----->
      | V         | |
      |---nombre_volumen---+---+----->
      '-FILE:--nombre_archivo-'

.-Replacedefs-----No-----+----->
>---+-----+-----><
  '-Replacedefs-----+No---+-'
      '-Yes-'

```

Parámetros

nombre_admin

Especifica los administradores para los que desea importar la información. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

Preview

Especifica si desea previsualizar el resultado de la operación de importación, sin importar la información de administrador. Este parámetro es opcional. Los siguientes valores de parámetro están soportados:

No

Especifica que se ha de importar la información.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información sobre el número y tipos de objetos importados, junto con el número de bytes transferidos se pasa a la consola del servidor y a los registros de actividades.

El valor predeterminado es NO. Si especifica YES en el valor, deberá montar los volúmenes de exportación.

DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

VOLumename (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Los siguientes valores de parámetro están soportados:

nombre_volumen









Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.

Para este dispositivo	Especifique
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsREMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

Replacedefs

Especifica si se sustituirán las definiciones de administrador ya existentes en el servidor de destino. Los siguientes valores de parámetro están soportados:

No

Especifica que no se sustituirán las definiciones.

Yes

Especifica que se sustituirán las definiciones.

El valor predeterminado es NO.

Ejemplo: importar información de administrador de volúmenes de cinta específicos

Desde el servidor, importar la información de todos los administradores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato:

```
import admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Ejemplo: importar información del administrador desde los volúmenes de cinta que se indican en un archivo

Desde el servidor, importe la información para todos los administradores definidos a los volúmenes de cintas que figuran en el archivo siguiente:

-  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA

Este archivo contiene estas líneas:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Emita el mandato:

 Sistemas operativos Linux

```
import admin devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import admin devclass=menu1 volumenames=file:tapevol.data
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con IMPORT ADMIN

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.

Mandato	Descripción
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT POLICY	Restaura información de políticas desde medio externo.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

IMPORT NODE (Importar información de nodos clientes)


Utilice este mandato para importar definiciones de nodos clientes desde un servidor o un medio secuencial a un servidor de IBM Spectrum Protect de destino.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Si especifica un dominio en el servidor de origen y si ese dominio de políticas también existe en el servidor de destino, los nodos importados se asocian con ese mismo dominio de políticas en el servidor de destino. De lo contrario, los nodos importados se asocian al dominio de políticas STANDARD en el servidor de destino.

Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Restricciones:

1. Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
2. No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.
3. Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores de destino deben estar configurados para las contraseñas de LDAP. Los datos que se importan desde un nodo que se autentica con un servidor de directorios LDAP no son accesibles si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos importados desde un nodo de LDAP todavía pueden seguir allí. Sin embargo, el servidor de destino debe estar configurado para que utilice LDAP con el fin de acceder a los datos importados.
4. Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
5. No se puede utilizar una clase de dispositivo CENTERA como el soporte de destino para un mandato de exportación, o como el medio de origen para un mandato de importación.
6. No se admite la importación o exportación incrementales de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
 - o Copias de seguridad de VMware donde deben transferirse periódica e incrementalmente copias de seguridad completas e incrementales a otro servidor.
 - o Grupos de copias de seguridad donde deben transferirse periódica e incrementalmente copias de seguridad completas y diferenciales a otro servidor.
 - o  Sistemas operativos Windows Datos de Windows System State que se transfieren periódica e incrementalmente a otro servidor.

La exportación/importación completa de estos datos a un nuevo sistema de archivos en el destino está soportada si se exporta el espacio de archivos completo que contiene los datos. Es decir, la exportación no debe utilizar las opciones *FILEDATA=ALLACTIVE*, *FROMDATE*, *TODATE* o *MERGEFILESPPACES*.

La práctica recomendada para transferir incrementalmente este tipo de datos entre dos servidores es utilizar la réplica de nodo.

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de importación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela un proceso subordinado IMPORT NODE, puede que algunos de los datos ya se hayan importado. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Para un servidor que tenga clientes que admitan Unicode, puede conseguir que el servidor convierta el nombre de espacio de archivos que especifique, o bien utilizar los parámetros siguientes:

- HEXFILESPACE
- UNIFILESACE

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>>IMPORT Node----->
| .-,-----|. |
| V          | |
|'---nombre_nodo+--'|

>----->
| .-,-----|. |
| V          | |
|'-FILESpace-----nombre_espacio_archivos+--'|

>----->
| .-,-----|. |
| V          | |
|'-HEXFILESpace-----nombre_espacio_archivos+--'|

>----->
| .-,-----|. |
| V          | |
|'-UNIFILESace-----nombre_espacio_archivos+--'|

>----->
| .-,-----|. |
| V          | |
|'-DOMAINS-----nombre_dominio+--'|

.-FILEData-----None----- .-Preview ----No-----
>----->
|'-FILEData-----+ALL-----+| |'-Preview-----+No--+|
|          +-None-----+ |          '-Yes-|
|          +-Archive-----+
|          +-Backup-----+
|          +-BACKUPActive-+
|          +-ALLActive----+
|          '-Spacemanged-|

>>>DEVclass-----nombre_clase_dispositivo----->

.-Dates-----Absolute-----
>----->
|'-Dates-----+Absolute+|
|          '-Relative-|

| .-,-----|. |
| V          | |
>>>VOLumenames-----+---nombre_volumen+----->
|'-FILE:--nombre_archivo-|

.-Replacedefs-----No-----
>----->
|'-Replacedefs-----+No--+|
|          '-Yes-|

.-MERGEfilespace-----No-----

```

```

>-----+----->
  '-MERGEfilespaces-----+No--+-'
                                '-Yes-'

.-PROXynodeassoc-----No-----
>-----+-----<
  '-PROXynodeassoc-----+No--+-'
                                '-Yes-'

```

Parámetros

nombre_nodo

Especifica los nodos cliente para los que desea importar la información. Este parámetro es opcional.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Se incluirán en la lista todos los nodos que coincidan.

FILESpace

Especifica los nombres de espacios de archivos para los que desea importar la información. Este parámetro es opcional. El valor predeterminado es especificar todos los espacios de archivos.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

Importante:

1. No se sustituirán los espacios de archivos existentes. Se crearán espacios de archivos nuevos cuando se encuentren nombres idénticos. Sin embargo, es posible que este nuevo nombre coincida con un nombre existente en el nodo de cliente que puede disponer de espacios de archivos de los que aún no se ha hecho una copia de seguridad en el servidor.
2. Sólo puede especificarse este parámetro para espacios de archivos que no son Unicode. Para importar todos los espacios de archivos Unicode y no Unicode, utilice el parámetro FILEDATA=ALL sin los parámetros FILESPACE y UNIFILESPACE.

DOmains

Especifica los dominios de políticas desde donde debe importarse información de nodos. Estos dominios deben estar incluidos en los datos exportados. Este parámetro es opcional. El valor predeterminado es especificar todos los dominios exportados.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

FILEData

Especifica el tipo de los archivos que deben importarse para todos los nodos encontrados en el medio de exportación. Este parámetro es opcional. El valor predeterminado es NONE.

Si está importando desde un medio secuencial, la clase de dispositivo que utilizan los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para importar la información del nodo. El límite de montaje para la clase de dispositivo debe ser como mínimo 2.

Las descripciones siguientes mencionan las copias de archivos de copia de seguridad *activas* e *inactivas*. Una copia de archivo de copia de seguridad activa es la copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás copias de archivo de copia de seguridad se denominan copias inactivas. Los valores que puede tener el parámetro son:

ALL

El servidor importa todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management. Los espacios de archivos que están incluidos son Unicode y no Unicode.

None

Sólo se importan las definiciones de nodos. El servidor no importa archivos.

ARchive

El servidor sólo importa las copias archivadas.

Backup

El servidor sólo importa las versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

El servidor sólo importa las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato IMPORT.

ALLActive

El servidor importa todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato IMPORT.

SPacemanaged

El servidor solo importa los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si se previsualiza el resultado de la operación de importación, sin importar la información. La opción PREVIEW=YES exige que se monten los volúmenes de exportación. Los valores siguientes están soportados:

No

Especifica que se ha de importar la información de nodos.

Yes

Especifica que desea previsualizar el resultado de la operación de importación, sin importar los archivos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

Este parámetro es opcional. El valor predeterminado es NO.

DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si al ejecutarse la importación todas las unidades para esta clase de dispositivo están ocupadas, el servidor cancela las operaciones de prioridad inferior, como por ejemplo, identificar duplicados, para que haya una unidad disponible.

Dates

Especifica si las fechas para las copias de archivos se establecen como la misma fecha cuando se exportaron los archivos, o se ajustan a la fecha de importación.

Este parámetro admite los valores siguientes:

Absolute

Las fechas de las copias de archivos se establecen en los valores especificados al exportarse los archivos.

Relative

Las fechas de las copias de archivos se ajustan a la fecha de importación.

El valor predeterminado es ABSOLUTE.

Si el medio de exportación está desocupado durante algún tiempo después de la exportación, por ejemplo, si permanece sobre una estantería durante seis meses, la copia original o las fechas de archivado pueden ser lo suficientemente antiguas como para desencadenar que las copias de archivo caduquen inmediatamente cuando los datos se importen a un servidor. La especificación RELATIVE de este valor se ajustará al tiempo transcurrido desde la exportación, de modo que las copias de los archivos no caduquen de forma inmediata.

Por ejemplo, supongamos que una cinta de exportación contiene una copia archivada realizada cinco días antes de la operación de exportación. Si el medio se ha guardado durante seis meses y luego se importa, el archivo de archivado aparecerá de forma predeterminada como insertada hace seis meses y cinco días (DATES=ABSOLUTE) y puede caducar inmediatamente dependiendo del valor de retención que se especifica en la clase de gestión del archivo. Especificando DATES=RELATIVE da como resultado el restablecimiento de la fecha de archivado para el archivo a hace cinco días durante la importación. De este modo, el parámetro DATES=RELATIVE ajusta las fechas de las copias archivadas y copias de seguridad en el tiempo transcurrido desde que se ha producido la operación de exportación.

VOLumenames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Los valores que puede tener el parámetro son:

nombre_volumen

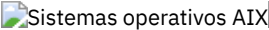


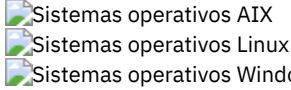
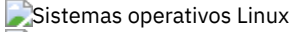
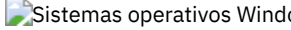
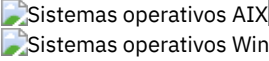
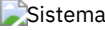

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
-----------------------	-------------

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	 Sistemas operativos AIX  Sistemas operativos Linux Cualquier serie de nombre de archivo cualificada al completo. Un ejemplo de ello es /imdata/mt1.  Sistemas operativos Windows Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo, d:\Archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

Replacedefs

Especifica si se sustituirán las definiciones del servidor destino. El valor predeterminado es NO. Los valores que puede tener el parámetro son:

No

Los objetos no se sustituyen.

Yes

Los objetos se sustituyen.

HEXFILESpace

Especifica la representación hexadecimal de los nombres de espacio de archivos en formato UTF-8. Puede separar varios nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Para visualizar la representación hexadecimal de un nombre de espacio de archivos, puede utilizar el mandato QUERY FILESPACE con FORMAT=DETAILED.

UNIFILESpace

Especifica que los espacios de archivos que son conocidos por el servidor están activados para Unicode. El servidor convierte los nombres que se especifican de la página de códigos del servidor a la página de códigos UTF-8 para encontrar los espacios de archivos que deben importarse. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizarse un carácter comodín para especificar un nombre. Este parámetro es opcional.

MERGEfilespaces

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

PROXynodeassoc

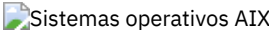

Especifica si se importan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.


Ejemplo: importar información de nodo cliente desde cintas

Desde el servidor, importar la información de nodo cliente de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import node devclass=menu1 volumenames=tape01,tape02,tape03
```



Ejemplo: importar información de nodo cliente desde las cintas que se indican en un archivo

 Sistemas operativos AIX  Sistemas operativos Linux
Desde el servidor, importar la información de nodo cliente desde los volúmenes de cinta listados en un archivo denominado TAPEVOL.

 Sistemas operativos Windows Desde el servidor, importar la información de nodo cliente desde los volúmenes de cinta listados en un archivo denominado TAPEVOL.DATA.

Este archivo contiene estas líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.  Sistemas operativos AIX
 Sistemas operativos Linux

```
import node devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import node devclass=menu1 volumenames=file:tapevol.data
```

Ejemplo: importar la copia de seguridad activa para un nodo cliente

Desde el servidor, importe las versiones de copia de seguridad activas de los datos de archivos para el nodo cliente JOE desde el volumen de cinta TAPE01. El espacio de archivos es Unicode.

```
import node joe unifilespace=\\joe\c$ filedata=backupactive  
devclass=menu1  
volumenames=tape01
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con IMPORT NODE

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT POLICY	Restaura información de políticas desde medio externo.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

IMPORT POLICY (Importar información de políticas)

Utilice este mandato para importar información de dominio de políticas del medio de exportación secuencial al servidor de IBM Spectrum Protect. Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Los datos de cliente de IBM Spectrum Protect se pueden traspasar entre servidores de mediante el proceso de exportación e importación, si ambas plataformas admiten el mismo tipo de medio extraíble.

Restricción:

1. Si los niveles del servidor de destino y origen no son compatibles, es posible que la operación de importación no funcione.
2. No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de importación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela el proceso subordinado IMPORT POLICY, ya están importados algunos datos. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-Import Policy-----*-----
| .-,-----|
| V          |
|'---nombre_dominio--+'
.
.-Preview ----No-----
>-----+----->
|'-Preview-----+No--+'
|'-Yes-'
.
>---DEVclass-----nombre_clase_dispositivo----->
| .-,-----|
| V          |
>---VOLumenames-----+---nombre_volumen+----->
|'-FILE:--nombre_archivo-'
.
.-Replacedefs-----No-----
>-----+-----<
|'-Replacedefs-----+No--+'
|'-Yes-'

```

Parámetros

nombre_dominio

Especifica los dominios de políticas para los que se va a importar la información. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. El valor predeterminado (*) son todas las políticas.

Preview

Especifica si desea previsualizar el resultado de la operación de importación sin importar la información. Este parámetro admite los valores siguientes:

No

Especifica que se ha de importar la información.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades.

La opción PREVIEW=YES exige que se monten los volúmenes de exportación. Este parámetro es opcional. El valor predeterminado es NO.

DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

VOLumenames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Este parámetro admite los valores siguientes:










nombre_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo: <ul style="list-style-type: none">•  Sistemas operativos AIX  Sistemas operativos Linux /imdata/mt1•  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsREMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

Replacedefs

Especifica si se sustituirán las definiciones de política del servidor destino. Este parámetro admite los valores siguientes:

Yes

Especifica que se han de sustituir los objetos por objetos importados.

No

Especifica que no se han de sustituir los objetos por objetos importados.

El valor predeterminado es NO.

Ejemplo: importar información de política desde volúmenes de cinta específicos

Desde el servidor, importar la información de todas las políticas definidas de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Ejemplo: importar información de política desde los volúmenes de cinta que se indican en un archivo

Desde el servidor, importe la información de todas las políticas definidas desde los volúmenes de cinta que se indican en un archivo denominado de la siguiente manera:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
- TAPEVOL.DATA

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
import policy devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import policy devclass=menu1 volumenames=file:tapevol.data
```

Tabla 1. Mandatos relacionados con IMPORT POLICY

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

IMPORT SERVER (Importar información del servidor)

Utilice este mandato para copiar toda o parte de la información de control del servidor y datos de archivo del cliente especificado del medio de exportación al servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Restricciones:

- Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
- No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.
- Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores de destino deben estar configurados para las contraseñas de LDAP. Los datos del servidor que se exportan desde un nodo que se autentica con un servidor de directorios LDAP no son accesible si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos exportados desde un nodo de LDAP todavía pueden seguir allí. Sin embargo, el servidor de destino debe estar configurado para que utilice LDAP con el fin de acceder a los datos.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
 - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.
 - Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
 - Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESPPACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

También puede iniciar un proceso de importación de la información del servidor y los datos de archivo de cliente directamente desde el servidor de origen. Para obtener más información, consulte los mandatos EXPORT.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. i se cancela un proceso subordinado IMPORT SERVER, parte de los datos ya se habrán importado. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las

bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los mandatos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-FILEData----None-----
>>-IMport Server-----+----->
      '-FILEData----+All-----+'
                        +-None-----+
                        +-ARchive-----+
                        +-Backup-----+
                        +-BACKUPActive-+
                        +-ALLActive----+
                        '-SPacemanaged-'

      .-Preview ----No-----
>-----+----->
      '-Preview----+No--+-'
                '-Yes-'

>--DEVclass----nombre_clase_dispositivo----->

      .-Dates----Absolute-----
>-----+----->
      '-Dates----+Absolute--+-'
                '-Relative-'

      .-,-----
      V          |
>--VOLumenames----+---nombre_volumen+----->
      '-FILE:--nombre_archivo-'

      .-Replacedefs----No-----
>-----+----->
      '-Replacedefs----+No--+-'
                '-Yes-'

      .-MERGEfilespace----No-----
>-----+----->
      '-MERGEfilespace----+No--+-'
                '-Yes-'

      .-PROXynodeassoc----No-----
>-----+----->
      '-PROXynodeassoc----+No--+-'
                '-Yes-'

```

Parámetros

FILEData

Especifica el tipo de archivos que deben importarse para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

La clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para importar la información. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las copias de archivos de copia de seguridad activas e inactivas. Una copia de archivo de copia de seguridad activa es la copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás copias de archivo de copia de seguridad se denominan copias inactivas. Este parámetro admite los valores siguientes:

ALL

IBM Spectrum Protect importa todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no importa archivos, sólo las definiciones de los nodos.

ARchive

IBM Spectrum Protect sólo importa las copias archivadas.

Backup

IBM Spectrum Protect sólo importa las versiones de copia de seguridad, ya sean versiones activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo importa las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato IMPORT.

ALLActive

IBM Spectrum Protect importa todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el mandato IMPORT.

SPacemanaged

IBM Spectrum Protect importa solo los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si se previsualiza el resultado de la operación de importación, sin importar la información. Este parámetro admite los valores siguientes:

No

Especifica que se ha de importar la información del servidor.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se transfiere a la consola del servidor y a las anotaciones de actividades.

Este parámetro es opcional. El valor predeterminado es NO. Si se especifica la opción PREVIEW=YES, deberá montar los volúmenes de exportación.

DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No se pueden especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

Dates

Especifica si las fechas para las copias de archivos se establecen como la misma fecha cuando se exportaron los archivos, o se ajustan a la fecha de importación.

Si el medio de importación está desocupado durante algún tiempo después de la exportación, por ejemplo, si permanece sobre una estantería durante seis meses, la copia original o las fechas de archivado pueden ser lo suficientemente antiguas como para desencadenar que las copias de archivo caduquen inmediatamente cuando los datos se importen a un servidor. La especificación RELATIVE de este valor se ajustará al tiempo transcurrido desde la exportación, de modo que las copias de los archivos no caduquen de forma inmediata.

Por ejemplo, supongamos que una cinta de importación contiene una copia archivada realizada cinco días antes de la operación de exportación. Si el medio de exportación se ha guardado durante seis meses y luego se importa, el archivo de archivado aparecerá de forma predeterminada como insertada hace seis meses y cinco días (DATES=ABSOLUTE) y puede caducar inmediatamente dependiendo del valor de retención que se especifica en la clase de gestión del archivo. Especificando DATES=RELATIVE da como resultado el restablecimiento de la fecha de archivado para el archivo a hace cinco días durante la importación. De este modo, el parámetro DATES=RELATIVE ajusta las fechas de las copias archivadas y copias de seguridad en el tiempo transcurrido desde que se ha producido la operación de exportación.

Este parámetro admite los valores siguientes:

Absolute

Las fechas de las copias de archivos se establecen en los valores especificados al exportarse los archivos.

Relative

La fecha de las copias de archivos se ajustan a la fecha de importación.

El valor predeterminado es ABSOLUTE.

VOLumenames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Este parámetro admite los valores siguientes:

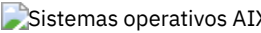
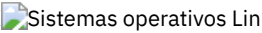
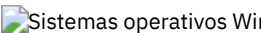
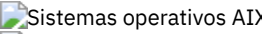
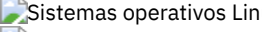
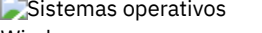
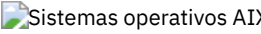
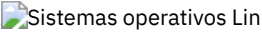
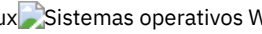
nombre_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	 Sistemas operativos AIX  Sistemas operativos Linux Cualquier serie de nombre de archivo o volumen cualificada al completo. Un ejemplo de ello es /imdata/mt1.  Sistemas operativos Windows Cualquier serie de nombre de archivo o volumen cualificada al completo. Por ejemplo, d:\Archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

Replacedefs

Especifica si se sustituirán los objetos del servidor. No se sustituirán los espacios de archivos existentes. Se crearán espacios de archivos nuevos cuando se encuentren nombres idénticos. Este parámetro admite los valores siguientes:

No

Especifica que no se han de sustituir los objetos por objetos importados.

Yes

Especifica que se han de sustituir los objetos por objetos importados.

El valor predeterminado es NO.

MERGEfilespace

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. No puede fusionar espacios de archivo no Unicode y Unicode de forma conjunta. Este parámetro admite los valores siguientes:

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino si existen espacios de archivos con el mismo nombre.

Yes

Especifica que los datos importados en el servidor de destino se agregan al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

El valor predeterminado es NO.

PROXynodeassoc

Especifica si se importan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

Ejemplo: importar información de todos los servidores definidos desde cintas específicas

Desde el servidor, importar la información de todos los servidores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: importar información de todos los servidores definidos desde cintas específicas y especificar que los archivos han de fusionarse en los espacios de archivos existentes

Desde el servidor, importar la información de todos los servidores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que un dispositivo asignado a la clase de dispositivo MENU1 pueda leer estos volúmenes de cinta y que los archivos de cliente se combinen en espacios de archivo del servidor destino si existen espacios de archivos de los mismos nombres.


```
import server devclass=menu1 volumenames=tape01,tape02,tape03
mergefilespace=yes
```

Ejemplo: importar información de todos los servidores definidos desde las cintas que se indican en un archivo

Desde el servidor, importar la información de todos los servidores definidos desde los volúmenes de cinta que se indican en el archivo denominado TAPEVOL. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo de entrada contiene estas líneas:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

Ejemplo: importar información de todos los servidores definidos desde las cintas que se indican en un archivo

Desde el servidor, importar la información de todos los servidores definidos desde los volúmenes de cinta que se indican en el archivo denominado TAPEVOL.DATA. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo de entrada contiene estas líneas:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol.data
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con IMPORT SERVER

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT POLICY	Restaura información de políticas desde medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

INSERT MACHINE (Insertar información de características o instrucciones de recuperación)

Utilice este mandato para agregar características de máquina cliente o instrucciones de recuperación a la información de la máquina existente en la base de datos.

Puede escribir un programa que lea los archivos que contienen la información y que genere los mandatos INSERT MACHINE adecuados.

Puede utilizar los mandatos QUERY para recuperar la información en caso de producirse un siniestro.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-INsert MACHine--machine_name--número_secuencia----->
>--+CHaracteristics--===texto-----+-----><
  '-RECOVERYInstructions--===texto-'
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina cliente.

número_secuencia (Necesario)

Especifica el número de secuencia de la línea de texto de la base de datos.

CHaracteristics

Especifica la información de las características de la máquina. Debe especificar las características o las instrucciones de recuperación, pero no las dos. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. El texto puede tener hasta 1024 caracteres.

RECOVERYInstructions

Especifica las instrucciones de recuperación. Debe especificar las características o las instrucciones de recuperación, pero no las dos. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. El texto puede tener hasta 1024 caracteres.

Ejemplo: actualizar la información de una máquina

Para la máquina DISTRICT5, insertar el texto de las características en la línea 1: "Machine owner is Mary Smith".

```
insert machine district5 1
characteristics="Machine owner is Mary Smith"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con INSERT MACHINE

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
QUERY MACHINE	Muestra información sobre máquinas.

Información relacionada:

[🔗](#) Especificación de información sobre las máquinas de nodos de cliente y de servidor

ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)

Utilice este mandato con el proceso de código de retorno en un script para emitir un mensaje desde un script del servidor para determinar dónde se encuentra el problema con un mandato del script.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

>>-ISSUE MESSAGE--*gravedad_mensaje*--*texto_mensaje*-----><

Parámetros

gravedad_mensaje (Obligatorio)

Especifica la gravedad del mensaje. Los indicadores de gravedad de mensajes son los siguientes:

- I Información. Se visualiza ANR1496I en el texto del mensaje.
- W Avisor. Se visualiza ANR1497W en el texto del mensaje.
- E Error. Se visualiza ANR1498E en el texto del mensaje.
- S Grave. Se visualiza ANR1499S en el texto del mensaje.

texto_mensaje (Obligatorio)

Especifica la descripción del mensaje.

Ejemplo: emitir un mensaje desde un script de servidor

Supongamos que tiene un script llamado `backupsript` que paraliza la base de datos de un cliente, toma una copia de seguridad de dicha base de datos y, a continuación reinicia la base de datos del cliente. A modo de ilustración, el script da como resultado un código de retorno distinto de cero. Utilice el mandato `ISSUE MESSAGE` con la gravedad del mensaje y el texto del mensaje. A continuación se muestra un ejemplo de un script de servidor que llama a `backupsript` en la máquina cliente y emite mensajes en función del código de retorno de `backupsript`.

```
issue message i "Starting backup"
define clientaction nodename action=command
objects="c:\backupsript" wait=yes
if (101) goto qfail
if (102) goto qwarn
if(103) goto backupf
if (104) goto restartf
issue message i "Backup of database complete"
exit
qfail: issue message e "Quiesce of database failed"
exit
warn: issue message w "Quiesce of database failed, taking fuzzy backup"

exit
backupf: issue message e "Backup of database failed"
exit
restartf: issue message s "Database restart failed"
exit
```

Mandato

```
issue message e "quiesce of database failed"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con `ISSUE MESSAGE`




Mandato	Descripción
<code>COPY SCRIPT</code>	Crea una copia de un script.
<code>DEFINE SCRIPT</code>	Define un script para el servidor de IBM Spectrum Protect.
<code>DELETE SCRIPT</code>	Suprime el script o líneas individuales del script.
<code>RENAME SCRIPT</code>	Redenomina un script con un nuevo nombre.
<code>RUN</code>	Ejecuta un script.
<code>UPDATE SCRIPT</code>	Cambia o añade líneas a un script.

LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)

Utilice este mandato para etiquetar volúmenes de cinta o, en una biblioteca automatizada, para etiquetar automáticamente los volúmenes a medida que se dan de alta. Con este mandato, servidor utiliza la etiqueta larga que, con frecuencia, los volúmenes llevan previamente etiquetada.

Restricción: Utilice este mandato sólo para las bibliotecas MANUAL, SCSI, ACSLS y 349X. El proceso del mandato no espera a que haya disponible una unidad, aunque la unidad está únicamente en estado IDLE. Si es necesario, puede hacer que una unidad de biblioteca esté disponible emitiendo el mandato DISMOUNT VOLUME para desmontar el volumen de esa unidad en particular. Cuando la unidad de biblioteca esté disponible, podrá volver a emitir el mandato LABEL LIBVOLUME.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

 Sistemas operativos AIX  Sistemas operativos Linux

Para utilizar el mandato LABEL LIBVOLUME, al menos debe existir una unidad que no se esté utilizando en ningún otro proceso de IBM Spectrum Protect. Esto incluye también los volúmenes que están montados. Si es necesario, utilice el mandato DISMOUNT VOLUME para desmontar el volumen desocupado, para que la unidad quede disponible.

De forma predeterminada, el mandato LABEL LIBVOLUME no graba encima de la etiqueta existente. Sin embargo, si desea grabar encima de una etiqueta existente, puede especificar la opción `OVERWRITE=YES`.

Atención:

- Cuando sobrescribe una etiqueta de volumen, destruye todos los datos en el volumen. Tenga cuidado al sobrescribir etiquetas de volumen para evitar la supresión de datos válidos.
- Las etiquetas en volúmenes VolSafe sólo pueden sobrescribirse una vez. Por lo tanto, utilice el mandato LABEL LIBVOLUME sólo una vez para los volúmenes VolSafe. Puede proteger la etiqueta contra la sobrescritura con la opción `OVERWRITE=NO` del mandato LABEL LIBVOLUME.

Si utiliza el mandato LABEL LIBVOLUME, puede identificar los volúmenes que deben etiquetarse de la siguiente manera:


- Nombre explícitamente un volumen.
- Especifique un intervalo de volúmenes utilizando el parámetro `VOLRANGE`.
- Utilice el parámetro `VOLLIST` para especificar un archivo que contenga una lista de nombres de volumen o para nombrar explícitamente uno o varios volúmenes.

En el caso de las bibliotecas automatizadas, se le pedirá que inserte el volumen en la ranura de entrada/salida de la biblioteca.

Cuando se habilita la entrada/salida virtual (VIO), los volúmenes que están en la estación de E/S ya no están en puertos de entrada ni de salida. Para asegurarse de que los volúmenes se pueden procesar, trasládelos de la estación de E/S a las ranuras VIO. Si no hay ninguna estación de conveniencia de E/S disponible, inserte el volumen en una ranura vacía.

En el caso de las bibliotecas manuales, se le pedirá que cargue el volumen directamente en una unidad.

Consejo: Para etiquetar automáticamente volúmenes de cinta, puede utilizar el parámetro `AUTOLABEL` en los mandatos `DEFINE LIBRARY` y `UPDATE LIBRARY`. Utilizando el parámetro `AUTOLABEL`, se evita tener que etiquetar previamente un conjunto de cintas. Este método es más eficaz que utilizar el mandato LABEL LIBVOLUME, que requiere montar los volúmenes por separado. Si utiliza el parámetro `AUTOLABEL` con una biblioteca SCSI, debe dar de alta las cintas especificando `CHECKLABEL=BARCODE` en el mandato `CHECKIN LIBVOLUME`. El parámetro `AUTOLABEL` toma de forma predeterminada el valor `YES` para todas las bibliotecas no SCSI y `NO` para bibliotecas SCSI.

 Sistemas operativos Windows

Para etiquetar los volúmenes con el mandato LABEL LIBVOLUME, especifique el parámetro `CHECKIN`.

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro `AUTOLABEL` en los mandatos `DEFINE LIBRARY` y `UPDATE LIBRARY`. Utilizando este parámetro, se evita tener que etiquetar previamente un conjunto de cintas. Este método también es más eficaz que utilizar el mandato LABEL LIBVOLUME, que requiere montar los volúmenes por separado. Si utiliza el parámetro `AUTOLABEL`, debe dar de alta las cintas especificando `CHECKLABEL=BARCODE` en el mandato `CHECKIN LIBVOLUME`.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows. IBM Spectrum Protect no proporciona programas de utilidad para dar formato o etiquetar estos tipos de soportes. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el mandato `label`.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis correspondiente a las bibliotecas manuales

```
>>-LABEL LIBVolume--nombre_biblioteca-----nombre_volumen----->
.-OVERWRITE-----No-----.-WAITTime----60----.
>+-----+-----+-----+-----+-----+-----><
'-OVERWRITE-----+No--+-' '-WAITTime----valor-'
        '-Yes-'
```

Sintaxis correspondiente a las bibliotecas SCSI

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>-----+nombre_volumen-----+----->
        '-SEARCH-----+Yes--| A |-----LABELSource-----+Barcode-----+-'
                '-Bulk--| A |-'                                '+-Prompt-----+
                                                                '-Vollist--| B |-'

                                .-OVERWRITE-----No-----.
>+-----+-----+-----+-----+-----+----->
'-CHECKIN-----+SCRatch-+-' '-OVERWRITE-----+No--+-'
        '-PRivate-'                                '-Yes-'

.-WAITTime----60----.
>+-----+-----+-----+-----+-----+-----><
'-WAITTime----valor-'

A (SEARCH=Yes, SEARCH=Bulk)

|--+VOLRange-----nombre_volumen1,nombre_volumen2--+-----|
|          .-,-----|
|          V          |
'-VOLList-----+nombre_volumen+-----+-----|
        '-FILE:--nombre_archivo-'

B (LABELSource=Vollist)

        .-,-----.
        V          |
|--VOLList-----+nombre_volumen+-----+-----|
        '-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas 349X

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>-----+nombre_volumen-----+----->
        '-SEARCH-----+Yes-----| A |-----'

                                .-OVERWRITE-----No-----.
>+-----+-----+-----+-----+-----+----->
'-CHECKIN-----+SCRatch-+-' '-OVERWRITE-----+No--+-'
        '-PRivate-'                                '-Yes-'

.-WAITTime----60----.
>+-----+-----+-----+-----+-----+-----><
'-WAITTime----valor-'

A (SEARCH=Yes)

|--+VOLRange-----nombre_volumen1,nombre_volumen2--+-----|
|          .-,-----|
|          V          |
'-VOLList-----+nombre_volumen+-----+-----|
```

```
'-FILE:--nombre_archivo-'
```

Sintaxis correspondiente a las bibliotecas ACSLS

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>----+--nombre_volumen-----+----->
      '-SEARCH-----Yes-----| A |----'
                                     .-OVERWRITE-----No-----.
>--+-----+-----+-----+----->
      '-CHECKIN-----+SCRatch+-'   '-OVERWRITE-----+No--+-'
      '-PRivate-'                   '-Yes-'

      .-WAITTime-----60----.
>--+-----+-----><
      '-WAITTime-----valor-'

A (SEARCH=Yes)

|---+--VOLRange-----+--nombre_volumen1,nombre_volumen2---+-----|
|          .-,-----|
|          V          |
|'-VOLList-----+--nombre_volumen+-----+'
|          '-FILE:--nombre_archivo-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que contiene el volumen de almacenamiento.

nombre_volumen

Especifica el nombre del volumen que debe etiquetarse.

- En bibliotecas SCSI: el servidor solicita que el volumen se inserte en una ranura en la biblioteca o, si está disponible, en un puerto de entrada/salida. El servidor identifica una ranura por la dirección de elemento de la ranura. Si está etiquetando un volumen en una biblioteca SCSI con varios puertos de entrada/salida, se etiquetará el volumen que tenga la ranura de número más bajo.

Aviso: Si especifica un nombre de volumen, el nombre que especifique sobrescribe la etiqueta impresa en el cartucho.

- En bibliotecas MANUAL: el servidor solicita que el volumen se inserte en una unidad.
- En bibliotecas 349X: el volumen puede encontrarse ya en la biblioteca, o se le puede solicitar que lo coloque en la estación de E/S.

Recuerde: Si el nombre de volumen especificado ya está definido en una agrupación de almacenamiento o en un archivo histórico de volúmenes, no se etiqueta el volumen y se visualiza un mensaje.

CHECKIN

Especifica si el servidor da de alta el volumen. Este parámetro es opcional. Los siguientes son los valores posibles:

SCRatch

Especifica que el servidor dará de alta los volúmenes y los agregará a la agrupación de reutilizables de la biblioteca. Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

PRivate

Especifica que el servidor dará de alta los volúmenes y los designará como privados. Los volúmenes privados sólo están disponibles al pedirlos por el nombre.

Si no especifica un valor para este parámetro, el mandato etiqueta el volumen, pero no lo incorpora. Si no especifica un valor para este parámetro y desea dar de alta el volumen, deberá emitir el mandato CHECKIN LIBVOLUME.

SEARCH

Especifica que el servidor busca en la biblioteca los volúmenes utilizables que deben etiquetarse. Este parámetro se aplica a las bibliotecas SCSI, 349X y ACSLS.

Son válidos los valores siguientes:

Yes

Especifica que el servidor sólo etiqueta volúmenes almacenados en la biblioteca, a menos que el volumen ya esté etiquetado o su código de barras no se pueda leer.

Si especifica la opción LABELSOURCE=PROMPT, el volumen se traslada a la unidad desde su ubicación en la biblioteca o en los puertos de entrada o en los de salida. El servidor le solicitará que emita el mandato REPLY que contiene la serie de etiqueta, y esa etiqueta se graba en la cinta.

Bulk

Especifica que el servidor busca en los puertos de entrada/salida de la biblioteca los volúmenes utilizables que deben etiquetarse. Esta opción sólo es válida para las bibliotecas SCSI.

Si especifica LABELSOURCE=BARCODE, se lee el código de barras del volumen. A continuación, la cinta se desplaza de su ubicación en la biblioteca o en los puertos de entrada/salida a una unidad en la que se graba la etiqueta del código de barras. Una vez etiquetada la cinta, se devuelve a su ubicación en la biblioteca, a los puertos de entrada/salida o a una ranura de almacenamiento si se especifica la opción CHECKIN. Para que el soporte para código de barras funcione correctamente en las bibliotecas admitidas en IBM Spectrum Protect, el servidor de IBM Spectrum Protect y el controlador de dispositivo deben estar en el mismo nivel. El soporte de código de barras está disponible en las bibliotecas admitidas por IBM Spectrum Protect y que utilizan el controlador de dispositivo de IBM Spectrum Protect o el controlador de dispositivo IBM® Magstar o LTO Ultrium.

Consejo: Se pueden utilizar los parámetros VOLRANGE o VOLLIST para limitar la búsqueda.

VOLRange

Especifica un rango de nombres de volúmenes separados con una coma. Utilice este parámetro para limitar la búsqueda de volúmenes para etiquetarlos cuando especifique SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca dentro del rango especificado, el mandato finalizará sin errores.

Sólo puede especificar los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Se etiquetan los 21 volúmenes: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Los 3 volúmenes se etiquetan: bar11a, bar12a, bar13a.
volrange=123400,123410	Se etiquetan los 11 volúmenes: 123400, 123401, ...123409, 123410.

VOLLlist

Especifica una lista de volúmenes. Utilice este parámetro para limitar la búsqueda de volúmenes para etiquetarlos cuando especifique SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca que se encuentren en la lista, el mandato finaliza sin errores. El parámetro VOLLIST también puede ser la fuente de nombres que se pueden utilizar para indicar volúmenes si el parámetro LABELSOURCE se define como VOLLIST. Si LABELSOURCE=VOLLIST, debe especificar el parámetro VOLLIST.

Son válidos los valores siguientes:

nombre_volumen

Especifica los nombres de uno o varios volúmenes que se utilizan para el mandato. Por ejemplo:

```
VOLLIST=TAPE01,TAPE02.
```

FILE:nombre_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el mandato. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar el volumen TAPE01, TAPE02 y TAPE03, cree un archivo denominado TAPEVOL que contenga las siguientes líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Puede especificar los volúmenes para el mandato según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Recuerde: El nombre de archivo es sensible a las mayúsculas/minúsculas.

LABELSource

Especifica si el servidor lee las etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo. Esta opción sólo es válida para las bibliotecas SCSI. Especifique este parámetro sólo cuando SEARCH=YES o SEARCH=BULK.

Puede especificar los valores siguientes:

Prompt

El servidor solicita los nombres de volumen necesarios.

Barcode

El servidor intenta leer la etiqueta del código de barras. Si no lo consigue, el servidor no etiqueta el volumen y muestra un mensaje.

Importante: Para que el soporte de código de barras funcione correctamente, deben instalarse los controladores de dispositivo adecuados para las bibliotecas.

Vollist

Esta opción sólo se aplica a las bibliotecas SCSI. El servidor intenta leer el archivo o la lista de archivos especificados. Si no lo consigue, el servidor no etiqueta los volúmenes y muestra un mensaje.

OVERWRITE

Especifica si el servidor intenta grabar encima de las etiquetas existentes. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta. Para los volúmenes StorageTek VolSafe, el valor debe ser NO.

Yes

Especifica que el servidor graba encima de las etiquetas existentes sólo si no se han definido aún ni la etiqueta existente ni la etiqueta solicitada o de código de barra en una agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

WAITTime

Especifica el número de minutos que el servidor esperará su respuesta o responderá a una petición. Especifique un valor dentro del rango de 0 a 9999. Si desea que el servidor le pregunte, especifique un tiempo de espera mayor que cero. El valor predeterminado es de 60 minutos. Por ejemplo, supongamos que el servidor le solicita que inserte una cinta en el puerto de entrada/salida de una biblioteca. Si ha especificado un tiempo de espera de 60 minutos, el servidor emite una petición y espera 60 minutos a que responda a la petición. De forma alternativa, supongamos que especifica 0 como tiempo de espera. Si ha insertado una cinta, un tiempo de espera cero dará lugar a que la operación continúe sin que se formule ninguna pregunta. Si no ha insertado una cinta, un tiempo de espera igual a cero hace que la operación falle.

Ejemplo: etiquetar automáticamente volúmenes de biblioteca

Etiquetar automáticamente las cintas de una biblioteca SCSI denominada AUTO a medida que incorpora los volúmenes.

```
label libvolume auto checkin=scratch search=yes labelsource=barcode  
overwrite=yes
```

Ejemplo: etiquetar volúmenes de biblioteca secuenciales

Etiquetar 3 volúmenes, de bar11a a bar13a, en una biblioteca SCSI denominada ABC. Cuando emita el siguiente mandato, los tres volúmenes se etiquetarán: bar11a, bar12a, bar13a.

```
label libvolume abc checkin=scratch search=yes volrange=bar11a,bar13a  
labelsource=barcode
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con LABEL LIBVOLUME

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.

Mandato	Descripción
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)

Utilice este mandato para cargar el conjunto predeterminado de desencadenantes de alertas en el servidor de IBM Spectrum Protect.

Para un servidor que se acaba de instalar, se define un conjunto predeterminado de mensajes para desencadenar las alertas. Puede modificar o suprimir los desencadenantes de alertas predeterminados. Utilice este mandato para completar las siguientes tareas:

- Cargar el conjunto predeterminado de desencadenantes de alertas y restaurar los que se hubieran suprimido.
- Sustituir todos los desencadenantes de alertas por el conjunto predeterminado original.

De forma predeterminada, este mandato no suprime los otros desencadenantes de alertas que se hayan creado, ni sustituye los desencadenantes de alertas predeterminados que se hayan modificado. Para suprimir todos los desencadenantes de alertas y restaurar el conjunto original de desencadenantes de alertas predeterminados, especifique RESET=yes.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-L0ad DEFALerttriggers--+-REset-----No-----+-----><
                          '-REset-----+No---+'
                          '-Yes-'

```

Parámetros

REset

Especifica si desea sustituir todos los desencadenantes de alertas por el conjunto predeterminado de desencadenantes de alertas. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que sólo se añaden los desencadenantes de alertas predeterminados. Los desencadenantes de alertas predeterminados originales se añaden al servidor. Los desencadenantes existentes no se suprimen. Si ya existe un desencadenante predeterminado en el servidor, no se sustituye ni se modifica.

Yes

Especifica que los desencadenantes de alertas se restauran a los valores predeterminados originales. Todos los desencadenantes de alertas se suprimen y, a continuación, se añaden el conjunto original de desencadenantes de alertas predeterminados.

Ejemplo: cargar los desencadenantes de alertas predeterminados en el servidor

Cargue los desencadenantes predeterminados para restaurar los que se han suprimido. Emita el mandato:

```
load defalertriggers
```

Ejemplo: sustituir todos los desencadenantes de alertas en el servidor por los desencadenantes de alertas predeterminados

Suprima todos los desencadenantes de alertas en el servidor y sustitúyalos por los valores predeterminados originales. Emita el mandato:

```
load defalertriggers reset=yes
```

Mandatos relacionados


```
lock node * authentication=local
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con LOCK NODE

Mandato	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.

LOCK PROFILE (bloquear un perfil)

Utilice este mandato en un gestor de configuración para bloquear temporalmente un perfil para que la información de configuración no se distribuya a los servidores gestionados suscritos.

Puede utilizar este mandato cuando esté realizando varias actualizaciones en la configuración y no desee distribuir esta información hasta que se hayan finalizado los cambios.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-LOCK PROFILE--nombre_perfil--+-60-----+-----><
                               '-minutos-'
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el perfil que se bloquea. Puede utilizar caracteres comodín para especificar varios nombres.

minutos

Especifica el tiempo, en minutos, que debe transcurrir para que IBM Spectrum Protect desbloquee el perfil de configuración. Especifique un entero de 0 a 10000. El valor predeterminado son 60 minutos. Si especifica 0, el perfil de configuración no se desbloqueará automáticamente. Utilice el mandato UNLOCK PROFILE para desbloquear el perfil antes de que transcurra el período de tiempo indicado o para desbloquearlo si ha especificado el valor 0. Este parámetro es opcional.

Ejemplo: bloquear un perfil durante un período de tiempo específico

Bloquear un perfil denominado DELTA durante 30 minutos.

```
lock profile delta 30
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con LOCK PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.

Mandato	Descripción
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

MACRO (Invocar una macro)

Utilice este mandato para invocar un archivo desde la línea de mandatos de administración que contiene uno o varios mandatos de administración de IBM Spectrum Protect que deben ejecutarse.

Restricción: Utilice este mandato sólo con clientes de línea de mandatos de administración.

Una macro es un archivo que contiene uno o varios mandatos de administración de IBM Spectrum Protect. Las macros sólo se pueden emitir desde el cliente de administración en las modalidades de proceso por lotes o interactiva. Las macros se almacenan como un archivo en la máquina (o sistema) cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

Crear una macro para entrar mandatos puede resultar muy útil si desea emitir mandatos que se utilizan reiteradamente, que contienen varios parámetros, o para procesar mandatos relacionados en un orden específico. Después de crear una macro, puede actualizar la información que contiene y volver a utilizarla, o puede copiar el archivo de macros, realizar cambios en la copia y, a continuación, ejecutar la copia.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-MACRO--nombre_macro--+-----+----->>
      | .------. |
      | v           | |
      |---substitution_value+--'
```

Parámetros

nombre_macro (Obligatorio)

Especifica el nombre de la macro.

substitution_value

Especifica el valor de una variable de sustitución en una macro. Si utiliza una variable de sustitución, puede volver a utilizar una macro siempre que necesite realizar la misma tarea para objetos diferentes o con valores de parámetro diferentes. Si desea especificar un valor que contenga espacios en blanco, debe encerrar el valor entre comillas. Este parámetro es opcional.

Ejemplo: crear una macro para registrar un nuevo administrador

Crear el archivo de macros denominado REGNG. Se utilizará la macro para inscribir y otorgar autorización a un nuevo administrador. Escriba la macro del siguiente modo:

```
/* Registrar y otorgar autorización a un nuevo administrador */
REGister Admin jones passwd          -
CONtactinfo="x1235"
GRant AUTHority jones                -
CLasses=Policy
```

Emita el siguiente mandato para ejecutar la macro:

```
macro regng.mac
```

Ejemplo: escribir una macro utilizando variables de sustitución

Crear el archivo de macros denominado AUTHRG, que contenga variables de sustitución, para inscribir y otorgar autorización a un nuevo administrador. Escriba la macro del siguiente modo:

```

/* Registrar y otorgar autorización a un nuevo administrador */
REGister Admin %1 %2 - /* Entrar id usuario y contraseña */
CONTACT=%3 /* Entrar infor. contacto (entre comillas, si es nec.) */
GRant AUTHority %1 - /* El servidor utiliza la variable */
- /* que ya ha definido */
CLasses=%4 /* Entrar la clase de privilegio */

```

Emita un mandato similar al siguiente, especificando los valores que desea pasar al servidor, para que el mandato se procese cuando se ejecute la macro.

```
macro authrg.mac jones passwd x1235 Policy
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con MACRO

Mandato	Descripción
COMMIT	Hace que los cambios en la base de datos sean permanentes.
ROLLBACK	Descarga cualquier cambio no confirmado en la base de datos desde que se ejecutó el último COMMIT.

Conceptos relacionados:

Macros de cliente administrativo

MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)

Utilice este mandato para migrar archivos de una agrupación de almacenamiento a la agrupación de almacenamiento siguiente de la jerarquía de almacenamiento.

Este mandato sólo puede utilizarse con agrupaciones de almacenamiento primarias. El formato de datos de la agrupación de almacenamiento no puede ser NETAPPDUMP, CELERRADUMP o NDMPDUMP. Los datos no se pueden migrar a o desde agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.

Sólo se permite un proceso de migración o reclamación para una agrupación de almacenamiento determinada en un momento dado. Si ya está ejecutándose un proceso de migración o reclamación para la agrupación de almacenamiento, no puede iniciar otro proceso de migración para la agrupación de almacenamiento.

Sólo debería utilizar este mandato si no utilizará la migración automática para la agrupación de almacenamiento. Para impedir que se ejecute la migración automática, establezca el atributo HIGHMIG de la definición de agrupación de almacenamiento en 100.

Si utiliza este mandato para iniciar un proceso de migración, pero la agrupación de almacenamiento no tiene identificada la siguiente agrupación de almacenamiento en la jerarquía, se activa un proceso de reclamación se activa para la agrupación de almacenamiento de origen. Para evitar el proceso de regeneración, defina la siguiente agrupación de almacenamiento en la jerarquía. A continuación, inicie el proceso de migración.

El mandato MIGRATE STGPOOL utiliza los valores de los siguientes parámetros en los mandatos DEFINE STGPOOL y UPDATE STGPOOL:

- MIGPROCESS
- MIGDELAY
- MIGCONTINUE
- NEXTPOOL
- LOWMIG

Consejo: Puede sustituir el valor del parámetro LOWMIG en los mandatos DEFINE STGPOOL y UPDATE STGPOOL especificando un valor para el parámetro LOWMIG en el mandato MIGRATE STGPOOL.

El mandato MIGRATE STGPOOL pasa por alto el valor del parámetro HIGHMIG de la definición de agrupación de almacenamiento. La migración se produce independientemente del valor del parámetro HIGHMIG.

Este mandato crea uno o varios procesos de migración que pueden cancelarse con el mandato CANCEL PROCESS. El número de procesos está limitado por el atributo MIGPROCESS de la definición de agrupación de almacenamiento. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Recuerde: La migración de datos de una agrupación de almacenamiento primaria configurada para eliminación de datos duplicados a otra agrupación de almacenamiento primaria que también está configurada para eliminación de datos duplicados elimina los datos duplicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado tanto en la agrupación de almacenamiento cuyos archivos se migrarán como en la agrupación de almacenamiento siguiente a la que se migrarán los archivos.

Sintaxis

```
>>-MIGrate STGpool--nombre_agrupación--+-----+----->
                                     '-LOWmig----número-'
                                     .-REclaim----No-----
>+-----+-----+-----+-----+-----+----->
  '-Duration----minutos-'  '-REclaim----+No--+-'
                              '-Yes-'

  .-Wait----No-----
>+-----+-----+-----+-----+-----+-----><
  '-Wait----+No--+-'
                    '-Yes-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento principal cuyos archivos se deben migrar.

DURation

Especifica el número máximo de minutos que se ejecuta la migración antes de cancelarse automáticamente. Al transcurrir el número de minutos especificado, el servidor cancelará automáticamente todos los procesos de migración para esta agrupación de almacenamiento. Los procesos finalizarán en cuanto detecten la cancelación automática. Como resultado, la migración puede ejecutarse durante más tiempo que el valor que especificó para este parámetro. Puede especificar un número de 1 a 9999. Este parámetro es opcional. Si no se especifica, el servidor se detendrá únicamente después de alcanzar el umbral inferior de migración.

LOWmig

Para agrupaciones de almacenamiento en disco de acceso secuencial y acceso aleatorio, especifica que la migración se debe detener cuando la cantidad de datos en la agrupación es igual o inferior a la capacidad estimada de este porcentaje de la agrupación. Este parámetro es opcional. El cálculo de las agrupaciones de almacenamiento en disco de acceso secuencial incluye la capacidad de todos los volúmenes reutilizables especificados para la agrupación. Dado que la migración se realiza por nodo o espacio de archivos, en función de la proximidad la ocupación de la agrupación de almacenamiento puede caer por debajo del valor especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0. En otros tipos de agrupaciones de almacenamiento de acceso secuencial, el servidor detiene la migración cuando el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento es igual o inferior a este porcentaje. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Puede especificar un número de 0 a 99 para este parámetro opcional. El valor predeterminado es el atributo LOWMIG de la definición de agrupación de almacenamiento.

REclaim

Especifica si se intenta la reclamación para la agrupación de almacenamiento antes de completar la migración. Sólo puede especificarse este parámetro para una agrupación de almacenamiento de acceso secuencial. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor no intentará una operación de reclamación antes de iniciar la migración.

Yes

Especifica que el servidor intentará una reclamación antes de iniciar la migración. La operación de reclamación se realizará para cualquier volumen de la agrupación de almacenamiento que satisfaga el umbral de reclamación especificado en el atributo RECLAIM de la definición de agrupación de almacenamiento antes de completar la migración. Si no hay ningún volumen que satisfaga el umbral de reclamación o si, tras la reclamación, el umbral LOWMIG no se ha alcanzado, el servidor iniciará la migración. Antes de reclamar espacio para las agrupaciones de almacenamiento definidas por RECLAMATIONTYPE=SNAPLOCK, el servidor suprime todos los volúmenes WORM FILE vacíos durante el proceso de reclamación que han excedido su periodo de reclamación.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si cancela este proceso, pueden haberse migrado ya algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando la operación finaliza. Los mensajes también se visualizan en las anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Nota: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: migrar una agrupación de almacenamiento a la siguiente agrupación de almacenamiento

Migrar datos de la agrupación de almacenamiento denominada BACKUPPOOL hasta la siguiente agrupación de almacenamiento. Especificar que el servidor debe finalizar la migración lo antes posible después de 90 minutos.


```
migrate stgpool backuppool duration=90
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con MIGRATE STGPOOL

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Visualiza información acerca de un proceso subordinado.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RECLAIM STGPOOL	Realiza una operación de reclamación para la agrupación de almacenamiento.


Información relacionada:

 Migración de archivos en una jerarquía de agrupaciones de almacenamiento

Mandatos MOVE

Utilice los mandatos MOVE para transferir datos de copia de seguridad o datos archivados entre agrupaciones de almacenamiento o bien para trasladar medios de recuperación ante siniestro al local o fuera del local.

- MOVE CONTAINER (Mover un contenedor)
- MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)
- MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)
- MOVE GRPMEMBER (Mover un miembro de grupo de servidores)
- MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)
- MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

MOVE CONTAINER (Mover un contenedor)

Utilice este mandato para mover el contenido de un contenedor de agrupación de almacenamiento a otro contenedor si se elimina un directorio de agrupación de almacenamiento o se daña un contenedor.

También puede utilizar este mandato para mover el contenido de un contenedor de agrupación de almacenamiento en estas condiciones:

- Cuando actualiza hardware
- Si se producen errores de E/S en un disco

Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

Sintaxis

```
>>-MOVE CONTainer--nombre_contenedor----->
>+-----+----->
  '-STGPOOLDIRectory---nombre_directorio-'
  .-Wait---Yes-----
>+-----+-----><
  '-Wait---+Yes+-'
      '-No--'
```

Parámetros

nombre_contenedor (Obligatorio)

Especifica el nombre del contenedor que se va a mover. Debe especificar el nombre completo de la vía de acceso del contenedor.

STGPOOLDIRectory

Especifica el nombre del directorio de agrupación de almacenamiento donde se mueve el contenedor. Este parámetro es opcional.

Si especifica un directorio de agrupación de almacenamiento, debe estar en la misma agrupación de almacenamiento que el contenedor original. El directorio de agrupación de almacenamiento se utiliza para el nuevo contenedor. Si no especifica un directorio de agrupación de almacenamiento, el servidor de IBM Spectrum Protect selecciona un directorio de agrupación de almacenamiento en la misma agrupación de almacenamiento.

Wait

Especifica si es necesario esperar a que el servidor de IBM Spectrum Protect termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. Especifique los siguiente valores:

No



El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

Yes


El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.

Ejemplo: mover un contenedor

 Sistemas operativos AIX  Sistemas operativos Linux Mueva el contenedor 0000000000000001.dcf del directorio de agrupación de almacenamiento /data1/storage/dir1 al directorio de agrupación de almacenamiento /data/storage/dir2.

```
move container /data1/storage/dir1/00/0000000000000001.dcf
stgpooldir=/data/storage/dir2
```

 Sistemas operativos Windows Mueva el contenedor 0000000000000001.dcf del directorio de agrupación de almacenamiento e:\data1\storage\dir1 al directorio de agrupación de almacenamiento e:\data\storage\dir2.

```
move container e:\data1\storage\dir1\00\0000000000000001.dcf
stgpooldir=e:\data\storage\dir2
```

Tabla 1. Mandatos relacionados con MOVE CONTAINER

Mandato	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
QUERY CONTAINER	Visualiza información sobre un contenedor.

MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)

Utilice este mandato para traspasar archivos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.

Restricción: No puede utilizar este mandato para volúmenes que están asignados a agrupaciones de almacenamiento de copias de contenedor.

Los archivos de un volumen de agrupación de almacenamiento primaria sólo se pueden traspasar a volúmenes de la misma agrupación de almacenamiento primaria o de una distinta. Los archivos de un volumen de agrupación de almacenamiento de copia sólo se pueden traspasar a volúmenes de la misma agrupación de almacenamiento de copia. Sólo puede traspasar archivos desde un volumen de agrupación de datos activos hasta los volúmenes de la misma agrupación de datos activos.

Además de trasladar datos desde los volúmenes de las agrupaciones de almacenamiento que tienen los formatos de datos NATIVE o NONBLOCK, este mandato también le permite trasladar datos desde los volúmenes de las agrupaciones de almacenamiento que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento de destino debe tener el mismo formato de datos que la agrupación de almacenamiento de origen. Si va a sacar datos de una agrupación de almacenamiento para actualizarse a la nueva tecnología de cintas, la agrupación de almacenamiento primaria de destino deberá asociarse a una biblioteca que tenga el nuevo dispositivo para las unidades de cinta. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

No puede trasladar datos de nodo a una agrupación o desde una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Si está desplazando archivos a volúmenes de la misma agrupación de almacenamiento, debe haber espacio suficiente en los volúmenes. De lo contrario, la operación no será satisfactoria.

Al traspasar archivos de un volumen de acceso secuencial, se necesitarán varios montajes de volumen de acceso secuencial para traspasar archivos que ocupan varios volúmenes.

Al traspasar archivos de un volumen de acceso aleatorio, el servidor borra todas las copias en caché de los archivos que hay en el volumen.

Después de haber finalizado una operación de traspaso de datos, es posible que un volumen no quede vacío si hay uno o varios archivos que no se pueden reubicar en otro volumen debido a errores de entrada/salida en el dispositivo, o si se han encontrado errores en el archivo. Si es necesario, puede suprimir el volumen con la opción de descartar todos los datos. Los archivos con errores de E/S o de otro tipo se suprimirán entonces.

Puede utilizar este mandato para traspasar archivos desde un volumen fuera del local de una agrupación de almacenamiento de copia o una agrupación de datos activos. Puesto que el volumen fuera del local no puede montarse, el servidor obtiene los archivos que se encuentran en el volumen fuera del local de una agrupación de almacenamiento primaria o de otra agrupación de almacenamiento de copia. A continuación, estos archivos se graban en los volúmenes de destino de la agrupación de almacenamiento de copia o la agrupación de datos activos original.

Durante el proceso de traslado de datos, las agrupaciones de datos activos no se pueden utilizar para obtener datos.

Si ejecuta el mandato MOVE DATA en un volumen fuera de local que contiene datos de proximidad, puede que sea necesario emitir el mandato MOVE DATA varias veces para trasladar todos los datos fuera del volumen. Por ejemplo, si está utilizando grupos de proximidad de espacio de archivos con un volumen fuera del local que contiene espacios de archivos en un grupo de proximidad y los espacios de archivos que no están en el grupo, debe emitir dos mandatos MOVE DATA. Cada mandato MOVE DATA traslada los datos para un solo grupo de archivos de proximidad o no de proximidad.

No utilice el mandato MOVE DATA si se está ejecutando un proceso de restauración (RESTORE STGPOOL o RESTORE VOLUME). Es posible que el mandato MOVE DATA cause que la restauración sea incompleta. Si emite el mandato MOVE DATA durante una operación de restauración y recibe un mensaje de error que indica que uno o más archivos están bloqueados y no se pueden trasladar, debe volver a emitir el mandato MOVE DATA después de realizarse la operación de restauración para trasladar los archivos restantes.

Recuerde:

La emisión de este mandato elimina datos duplicados al:

- Mover datos de una agrupación de almacenamiento primaria configurada para eliminación de datos duplicados a otra agrupación de almacenamiento primaria que también está configurada para la eliminación de duplicados.
- Mover datos dentro de una agrupación de almacenamiento de copia configurada para la eliminación de datos duplicados.
- Mover datos dentro de una agrupación de datos activos configurada para eliminación de datos duplicados.

Un volumen en una agrupación de almacenamiento cuyos duplicados se han eliminado puede contener archivos que se han suprimido lógicamente pero continúan enlazados con archivos en otros volúmenes. Si utiliza el mandato MOVE DATA para mover el contenido de un volumen de agrupación de almacenamiento cuyos duplicados se han eliminado a una agrupación de almacenamiento cuyos duplicados no se han eliminado, los archivos suprimidos de forma lógica no se graban en el nuevo volumen, ya que no existen lógicamente. Los archivos suprimidos se mantienen en los volúmenes originales para que otros archivos puedan hacer referencia a ellos. El proceso de MOVE DATA finaliza correctamente, pero ninguno de los archivos suprimidos se mueve al nuevo volumen de destino y el volumen de origen no se suprime. Puede emitir el mandato QUERY CONTENT con el parámetro FOLLOWLINKS=YES o FOLLOWLINKS=JUSTLINKS para verificar si el volumen contiene archivos enlazados con archivos en otros volúmenes.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento a la que pertenece el volumen y también para la nueva agrupación de almacenamiento, si se especifica una.

Sintaxis

```
>>-MOVE Data--nombre_volumen----->
>--+-----+----->
  '-STGpool-----nombre_agrupación-'
. -SHREDTONoshred----No----- .
>--+-----+----->
  '-SHREDTONoshred----+No--+-'
                               '-Yes-'

                               (1) (2)
. -RECONstruct-----No o Yes----- . -Wait-----No----- .
>--+-----+-----+----->>
  '-RECONstruct-----+No--+-' '-Wait-----+No--+-'
                               '-Yes-'                               '-Yes-'
```

Notas:

1. El valor predeterminado es NO si la agrupación de almacenamiento de origen o de destino es de acceso aleatorio. El valor predeterminado es YES si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial.
2. Este parámetro no está disponible o se pasa por alto en el caso de que el formato de datos sea NETAPPDUMP, CELERRADUMP o NDMPDUMP.

Parámetros

nombre_volumen (Necesario)

Especifica el volumen de agrupación de almacenamiento desde el que se traspasan los archivos.

STGpool

Especifica la agrupación de almacenamiento primaria a la que desea traspasar los archivos (la agrupación de almacenamiento de destino). Este parámetro es opcional y sólo se aplica a los datos que se traspasan de volúmenes de agrupaciones de almacenamiento primarias. Si no especifica un valor para este parámetro, los archivos se desplazarán a otros volúmenes en la misma agrupación de almacenamiento.

SHREDTONoshred

Especifica si los datos se trasladan de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no permitirá que se traspasen datos de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Si la agrupación de almacenamiento de origen implementa la destrucción de datos y la agrupación de almacenamiento de destino no existe, la operación falla.

Yes

Especifica que el servidor permite que se trasladen datos de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Los datos de origen se destruirán cuando la operación se haya completado. Los datos de destino no se destruirán cuando se supriman.

RECONstruct

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de un conjunto. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO. El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento.

Los valores posibles son:

No

Especifica que la reconstrucción de agregaciones de archivos no se ha completado durante el traslado de datos.

Yes

Especifica que la reconstrucción de agregaciones de archivos se ha completado durante el traslado de datos. Sólo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso en segundo plano en el registro de actividad o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano MOVE DATA, es posible que algunos archivos ya se hayan trasladado antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: traspasar archivos de un volumen de agrupación de almacenamiento

Traspasar los archivos del volumen de agrupación de almacenamiento STGVOL.1 a cualquiera de los volúmenes disponibles asignados a la agrupación de almacenamiento 8MMPPOOL.

```
move data stgvol.1 stgpool=8mmpool
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con MOVE DATA

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.

Mandato	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.

MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)

Utilice este mandato para hacer el seguimiento de los volúmenes que se van a trasladar fuera del local y para identificar los volúmenes caducados o vacíos que se van a trasladar al local. Puede hacer un seguimiento de los volúmenes de copia de seguridad de base de datos y de los volúmenes de agrupaciones de almacenamiento de copia de contenedor y de agrupaciones de almacenamiento de datos activos.

El proceso de volúmenes por parte de este mandato depende del uso que se les de:

Copias de seguridad de la base de datos del servidor

Para controlar si el mandato procesa volúmenes de copia de seguridad de base de datos, utilice el parámetro SOURCE en este mandato. El mandato puede procesar volúmenes utilizados para copias de seguridad de base de datos completas más las incrementales o de instantáneas. No se pueden especificar volúmenes virtuales (objetos de copia de seguridad almacenados en otro servidor). Puede modificar los volúmenes mediante cada estado, o bien utilizar el parámetro TOSTATE y omitir los estados para simplificar los traslados.

Agrupaciones de almacenamiento de copia

El mandato MOVE DRMEDIA siempre procesa volúmenes de agrupación de almacenamiento de copia.

Agrupaciones de almacenamiento de copia de contenedor

De forma predeterminada, los volúmenes de agrupación de almacenamiento de copia de contenedor no se pueden elegir para que las procese el mandato MOVE DRMEDIA. Para procesar volúmenes de agrupación de almacenamiento de copia de contenedor, debe emitir primero el mandato SET DRMCOPYCONTAINERSTGPOOL o especificar el parámetro COPYCONTAINERSTGPOOL en el mandato MOVE DRMEDIA.

Agrupaciones de almacenamiento de datos activos

De forma predeterminada, los volúmenes de agrupación de almacenamiento de datos activos no se pueden elegir para que las procese el mandato MOVE DRMEDIA. Para procesar volúmenes de agrupación de datos activos, debe emitir primero el mandato SET DRMACTIVEDATASTGPOOL o especificar el parámetro ACTIVEDATASTGPOOL en el mandato MOVE DRMEDIA.

Puede utilizar el mandato QUERY ACTLOG para comprobar si el mandato MOVE DRMEDIA se ha ejecutado correctamente. También puede ver esta información desde la consola del servidor.

Restricción: No ejecute los mandatos MOVE DRMEDIA y BACKUP STGPOOL simultáneamente. Asegúrese de que los procesos de copia de seguridad de agrupación de almacenamiento se han completado antes de emitir el mandato MOVE DRMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO privilegio de operador, de almacenamiento sin restricciones o de sistema.
- Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES (el valor predeterminado): privilegio de sistema.

Sintaxis

```
>>-MOVE DRMedia--nombre_volumen----->
>--+-----+----->
  '-WHEREState--==--MOUNTable-----+'
      +-NOTMOUNTable----+
      +-COUrier-----+
      +-VAULTRetrieve---+
```

```

'-COURIERRetrieve-'
>----->
'-BEGINDate---fecha-' '-ENDDate---fecha-'
>----->
'-BEGINTime---hora-' '-ENDTime---hora-'
>----->
'-COPYContainerstgpool---nombre_agrupación-'
>----->
'-COPYstgpool---nombre_agrupación-'
>----->
'-ACTIVEDatastgpool---nombre_agrupación-'
.-Source---DBBackup-.
>----->
'-Source---DBBackup-'
      +-DBSnapshot+
      +-DBNone----'
.-REMove---Bulk-.
>----->
'-REMove---No-'
      +-Yes-----+
      +-Bulk-----+
      '-Untileefull-'
>----->
'-TOSTate---NOTMOUNTable-'
      +-COURier-----+
      +-VAult-----+
      +-COURIERRetrieve+
      '-ONSITERetrieve--'
>----->
'-WHERELocation---location-'
>----->
'-TOLocation---location-' '-CMD---"mandato"'
.-APPend---No-.
>----->
'-CMDFilename---nombre_archivo-' '-APPend---No-'
      '-Yes-'
.-Wait---No-.
>-----<
'-Wait---No-' '-CAP---x,y,z-'
      '-Yes-'

```

Parámetros

nombre_volumen (Necesario)

Especifica el nombre del volumen que se ha de procesar. Puede utilizar caracteres comodín. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE. El servidor busca nombres coincidentes de entre los siguientes volúmenes seleccionables:

- Volúmenes de copia de seguridad de base de datos, según lo especificado por el parámetro SOURCE de este mandato.
- Volúmenes de la agrupación de almacenamiento de copia de las agrupaciones de almacenamiento especificadas en el parámetro COPYSTGPOOL. Si no utiliza el parámetro COPYSTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de copia que se especificaron anteriormente en el mandato SET DRMCOPYSTGPOOL.
- Volúmenes de agrupación de almacenamiento de copia de contenedor de las agrupaciones de almacenamiento nombradas en el parámetro COPYCONTAINERSTGPOOL. Si no utiliza el parámetro COPYCONTAINERSTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de copia de contenedor que se especificaron anteriormente en el mandato SET DRMCOPYCONTAINERSTGPOOL.
- Los volúmenes de agrupación de almacenamiento de datos activos de las agrupaciones de almacenamiento nombradas en el parámetro ACTIVEDATASTGPOOL. Si no utiliza el parámetro ACTIVEDATASTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de datos activos que se especificaron anteriormente en el mandato SET DRMACTIVEDATASTGPOOL.

El resto de parámetros también pueden limitar los resultados del mandato.

WHEREState

Especifica el estado de los volúmenes que se han de procesar. Este parámetro es necesario si no se especifica TOSTATE o bien si se utiliza un carácter comodín para el nombre del volumen. Para obtener más información, consulte la Tabla 2 y la Tabla 3.

Especifique uno de los siguientes valores:

MOutable

Estos volúmenes contienen datos válidos y están disponibles para procesos en local. Los valores cambian a NOTMOUNTABLE si no se especifica el parámetro TOSTATE.

En función del comportamiento del parámetro REMOVE puede que el servidor expulse los volúmenes de una biblioteca automatizada antes de cambiar el estado del destino.

En el caso de las bibliotecas externas, el servidor envía peticiones al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas.

NOTMOutable

Estos volúmenes están en el local, contienen datos válidos y no están disponibles para procesos en el local. Los valores cambian a COURIER si no se especifica el parámetro TOSTATE.

COURier

Estos volúmenes están con el transportista y se trasladan fuera del local. Los valores solo cambian a VAULT.

VAULTRetrieve

Estos volúmenes se encuentran en la cámara de seguridad fuera del local y no contienen datos válidos. Los valores cambian a COURIERRETRIEVE si no se especifica el parámetro TOSTATE.

COURIERRetrieve

Estos volúmenes están con el transportista y se trasladan al local. Los valores solo cambian a ONSITERETRIEVE. El servidor elimina de la base de datos los registros de los volúmenes de agrupación de almacenamiento de copia reutilizable y de copia de seguridad de base de datos.

BEGINDate

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha más antigua en la que existe información del volumen. Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/1998
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY-7 o -7 Para identificar los volúmenes que se han cambiado al estado actual hace una semana, puede especificar TODAY-7 o -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDDate

Especifica la fecha final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con anterioridad a la fecha especificada. El valor predeterminado es la fecha actual.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/1998

Valor	Descripción	Ejemplo
TODAY	La fecha actual.	TODAY Para identificar los volúmenes que se han cambiado al estado actual hoy, especifique TODAY.
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-1 o -1 Para identificar los volúmenes que se han cambiado al estado actual hace una semana, puede especificar TODAY-1 o -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial utilizada para seleccionar volúmenes para su proceso. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada con el parámetro BEGINDATE.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	12:33:28
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-03:30 o -03:30 Si emite el mandato MOVE DRMEDIA a las 9:00 con BEGINTIME=NOW-03:30 o BEGINTIME=-03:30, el servidor identifica los volúmenes que se han cambiado a su estado actual a las 05:30 en la fecha de inicio que ha especificado.

ENDTime

Especifica la hora final utilizada para seleccionar volúmenes para su proceso. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado son las 23:59:59.

Puede especificar la hora utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	12:33:28
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00 Si emite el mandato MOVE DRMEDIA a las 9:00 con ENDTIME=NOW+03:30 o ENDTIME=+03:30, el servidor identifica los volúmenes que se han cambiado a su estado actual a las 12:30 en la fecha de finalización que ha especificado.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30

COPYContainerstgpool

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de almacenamiento de copia de contenedor que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento especificadas con el mandato SET DRMCOPYCONTAINERSTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYCONTAINERSTGPOOL se ha emitido anteriormente con nombres de agrupación de almacenamiento de copia de contenedor, el servidor procesa solo esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYCONTAINERSTGPOOL o si todas las agrupaciones de almacenamiento de copia de contenedor se han eliminado mediante el mandato SET DRMCOPYCONTAINERSTGPOOL, el servidor procesa todos los volúmenes de agrupación de almacenamiento de copia de contenedor en función de la configuración del parámetro WHERESTATE. Si el parámetro se establece en un valor NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE, los volúmenes se procesan. Si el valor es MOUNTABLE, los volúmenes no se procesan.

COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de almacenamiento de copia que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento de copia especificadas con el mandato SET DRMCOPYSTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYSTGPOOL, o si se han eliminado todas las agrupaciones de almacenamiento de copia utilizando el mandato SET DRMCOPYSTGPOOL, el servidor procesará todos los volúmenes de agrupación de almacenamiento de copia que se encuentren en el estado especificado. Los estados disponibles son MOUNTABLE, NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE.

ACTIVEDatastgpool

Especifica el nombre de la agrupación de datos activos cuyos volúmenes van a procesarse. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de datos activos que se han especificado con este parámetro alteran temporalmente las agrupaciones de almacenamiento de datos activos que se han especificado con el mandato SET DRMACTIVEDATASTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si el mandato SET DRMACTIVEDATASTGPOOL se emitió anteriormente con nombres de agrupaciones de datos activos válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMACTIVEDATASTGPOOL, o se han eliminado todas las agrupaciones de almacenamiento de copia utilizando el mandato SET DRMACTIVEDATASTGPOOL, el servidor procesa todos los volúmenes de agrupación de datos activos en el estado especificado. Los estados disponibles son NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE. Los volúmenes que se encuentran en el estado MOUNTABLE no se procesarán.

Source

Especifica que se han de incluir los volúmenes de copia de seguridad de base de datos para su proceso. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Especifique uno de los siguientes valores:

DBBackup

Especifica que el servidor incluye volúmenes de copia de seguridad de base de datos completa e incremental para su proceso.

DBSnapshot

Especifica que el servidor incluye volúmenes de copia de seguridad de instantánea de base de datos para su proceso.

DBNone

Especifica que el servidor no incluye ningún volumen de copia de seguridad de base de datos para su proceso.

REMove

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles son YES, NO, BULK y UNTILEEFULL. El valor predeterminado es BULK. La respuesta del servidor a cada valor y el valor predeterminado depende del tipo de biblioteca.
 Restricción: Solo puede utilizar la opción REMOVE=UNTILEEFULL con el tipo de biblioteca SCSI.

Bibliotecas SCSI

La respuesta del servidor al mandato depende de si la biblioteca tiene puertos de entrada/salida y, si es así, de si hay un puerto disponible para su uso. Consulte la tabla siguiente.

Tabla 1. Respuesta del servidor para bibliotecas SCSI

Característica de biblioteca	Respuesta del servidor cuando se especifica REMOVE=YES	Respuesta del servidor cuando se especifica REMOVE=BULK	Respuesta del servidor cuando se especifica REMOVE=NO	Respuesta del servidor cuando se especifica REMOVE=UNTILEEFULL
La biblioteca no tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
La biblioteca tiene puertos de entrada/salida y un puerto de entrada/salida está disponible	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El servidor especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.
La biblioteca tiene puertos de entrada/salida, pero no hay puertos disponibles	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor espera que un puerto se haga disponible.	El servidor especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El mandato falla y los volúmenes elegibles restantes no se procesan. Haga que el puerto esté disponible y emita el mandato de nuevo.

Bibliotecas 349X

REMOVE=YES

El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.

REMOVE=BULK

El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.
REMOVE=NO

El gestor de biblioteca 3494 no expulsa el volumen. El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

Bibliotecas ACSLS

REMOVE=YES o REMOVE=BULK

El servidor expulsa el cartucho en la estación de E/S que convenga.

El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.

Mientras tiene lugar el traspaso de volúmenes del estado MOUNTABLE cuando se ha especificado REMOVE=YES, el mandato MOVE MEDIA utiliza más de una ranura del CAP para una biblioteca StorageTek que dispone de software ACSLS.

REMOVE=NO

El servidor no expulsa el cartucho.

El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

Bibliotecas externas

Puede especificar REMOVE=YES, REMOVE=BULK o REMOVE=NO. Para cualquier valor el servidor necesita que el gestor de biblioteca externo expulse el volumen de la biblioteca.

El hecho de que el volumen se expulse de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

TOSTate

Especifica el estado destino de los volúmenes que están procesándose. Este parámetro es necesario si el parámetro WHERESTATE no se ha especificado. Si especifica el parámetro TOSTATE, pero no el parámetro WHERESTATE, debe especificar el nombre del volumen. Los caracteres comodín no están permitidos. Consulte los apartados Tabla 2 y Tabla 3. Especifique uno de los siguientes valores:

NOTMOUNTABLE

Especifica que los volúmenes se cambiarán al estado NOTMOUNTABLE. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE.

Si los volúmenes están en la biblioteca automática, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado NOTMOUNTABLE, en función del comportamiento del parámetro REMOVE.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

COURIER

Especifica que los volúmenes se cambiarán al estado COURIER. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE o NOTMOUNTABLE.

En función del comportamiento del parámetro REMOVE y de si los volúmenes se encuentran en una biblioteca automatizada, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado COURIER.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

VAULT

Especifica que los volúmenes se cambiarán al estado VAULT. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE, NOTMOUNTABLE o COURIER.

En función del comportamiento del parámetro REMOVE y de si los volúmenes se encuentran en una biblioteca automatizada, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado VAULT.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas.

Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

COURIERRetrieve

Especifica que los volúmenes se cambiarán al estado COURIERRETRIEVE. Este valor sólo es válido si los volúmenes están en el estado VAULTRETRIEVE.

ONSITERtrieve

Especifica que los volúmenes se cambiarán al estado ONSITERRETRIEVE. Este valor sólo es válido si los volúmenes están en el estado VAULTRETRIEVE o COURIERRETRIEVE. Para los volúmenes de agrupaciones de almacenamiento de copia reutilizables y de copia de seguridad de la base de datos que se cambian al estado ONSITERRETRIEVE, el servidor suprime de la base de datos los registros de los volúmenes.

WHERELocation

Especifica la ubicación actual de los volúmenes. Este parámetro es opcional. La longitud máxima de la lista de la ubicación es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

TOLocation

Especifica la ubicación destino de los volúmenes. Este parámetro es opcional. La longitud máxima de la ubicación especificada es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Si no especifica la ubicación de destino, se utilizará la ubicación que define el mandato SET DRMNOTMOUNTABLE.

CMd

Especifica el mandato que se emitirá para cada volumen procesado con el mandato MOVE DRMEDIA. DRM graba los mandatos en un archivo que especifica el parámetro CMDFILENAME. Una vez finalizada la operación MOVE DRMEDIA, se pueden emitir los mandatos en el archivo. El mandato puede contener hasta 255 caracteres. Si el mandato contiene más de 240 caracteres, se divide en varias líneas y se añaden caracteres de continuación (+). Es posible que necesite alterar el carácter de continuación en función del sistema operativo. Este parámetro es opcional.

mandato

La serie de los mandatos debe estar encerrada entre comillas. La serie no debe contener comillas intercaladas. Por ejemplo, el parámetro CMD siguiente es válido:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

El ejemplo siguiente no es una forma válida de especificar el parámetro CMD:

```
cmd=""checkin libvol lib8mm" &vol status=scratch""
```

El mandato puede incluir variables de sustitución. Las variables no son sensibles a las mayúsculas y minúsculas, y no deben contener espacios en blanco detrás del símbolo &. Puede especificar los valores siguientes:

&VOL

Un nombre de volumen.

&LOC

Una ubicación de volumen.



&VOLDSN

El nombre de archivo que se debe grabar en las etiquetas de los medios de acceso secuencial. Por ejemplo, si la clase de dispositivo aplicable establece BKP como el prefijo del volumen de cinta, un nombre de archivo del volumen de cinta de la agrupación de almacenamiento de copia podría ser BKP.BFS y un nombre de archivo del volumen de cinta de copia de seguridad de la base de datos podría ser BKP.DBB.

&NL

El carácter de nueva línea. Cuando se utiliza un nuevo carácter de línea, el mandato se divide en la variable &NL. Si es necesario, debe especificar el carácter de continuación adecuado antes de &NL. Si no se especifica el carácter &NL y la línea de mandatos es superior a 240 caracteres, la línea se divide en varias líneas y se añaden los caracteres de continuación (+).


Sistemas operativos AIX Sistemas operativos Linux

 Sistemas operativos AIX  Sistemas operativos Linux
Especifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados mediante el parámetro CMD. Este parámetro es opcional.

Si no especifica un nombre de archivo o si especifica una serie nula (""), DRM utilizará el nombre de archivo que especifica el mandato SET DRMCMDFILENAME. Si no especifica un nombre de archivo con el mandato SET DRMCMDFILENAME, DRM generará un nombre de archivo añadiendo `exec.cmds` al nombre de ruta de directorio del directorio de trabajo actual del servidor.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

Sistemas operativos Windows

 Sistemas operativos Windows
Especifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados mediante el parámetro CMD. Este parámetro es opcional.

La longitud máxima del nombre de archivo son 259 caracteres. Si no especifica un nombre de archivo o si especifica una serie nula (""), DRM utilizará el nombre de archivo que especifica el mandato SET DRMCMDFILENAME. Si no se especifica un nombre de archivo con el mandato SET DRMCMDFILENAME, DRM genera un nombre de archivo uniendo `exec.cmd` al directorio que representa esta instancia del servidor (por lo general, el directorio desde el que se ha instalado el servidor). El DRM asigna el nombre de archivo especificado o generado. Si existe el nombre de archivo, DRM intenta utilizarlo; los datos existentes quedan sobregabados. Si ocurre esto y los mandatos ejecutables del archivo no se han ejecutado, emita el mandato QUERY DRMEDIA para volver a crear los mandatos ejecutables para la transición de volumen y la fecha deseadas.

Si el mandato MOVE DRMEDIA no se ha ejecutado correctamente y no se ha grabado ninguna de las series de mandatos especificadas con el parámetro CMD para el volumen que se ha traspasado correctamente, el nombre de archivo asignado se suprime. .

APPend

Especifica si se graba encima del contenido existente del archivo de mandatos o se añaden los mandatos al archivo. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No

DRM graba encima del contenido del archivo.

Yes

DRM agrega los mandatos al archivo.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para ver si la operación se ha realizado correctamente, emita el mandato QUERY ACTLOG.

Yes

Especifica que el servidor procesa este mandato en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra a continuación los mensajes de salida en el cliente de administración.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

x

El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.

y

El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.

z

El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

Reglas para estados y ubicaciones de destino

La siguiente tabla muestra cómo DRM determina el estado de destino y la ubicación de un volumen.

Estado de destino

- El valor del parámetro TOSTATE que se ha especificado.
- El estado siguiente del parámetro WHERESTATE que se ha especificado, si no se ha especificado el parámetro TOSTATE.

Ubicación destino

- El valor del parámetro TOLOCATION que se ha especificado.
- La ubicación del parámetro TOSTATE que se ha especificado, si no se ha especificado el parámetro TOLOCATION.
- La ubicación del estado siguiente del parámetro WHERESTATE que se ha especificado, si no se han especificado los parámetros TOLOCATION y TOSTATE.

Tabla 2. Destino y ubicación de volumen

Parámetros especificados	Estado de destino	Ubicación destino
WHERESTATE	El estado siguiente de WHERESTATE	Ubicación del estado siguiente
WHERESTATE, TOSTATE	TOSTATE	Ubicación de TOSTATE
WHERESTATE, TOLOCATION	El estado siguiente de WHERESTATE	TOLOCATON
WHERESTATE, TOSTATE, TOLOCATION	TOSTATE	TOLOCATION
TOSTATE	TOSTATE	Ubicación de TOSTATE
TOSTATE, WHERELOCATION	TOSTATE	Ubicación de TOSTATE
TOSTATE, WHERELOCATION, TOLOCATION	TOSTATE	TOLOCATION

Reglas para transiciones de estado

Las tablas siguientes muestran las transiciones de estado que pueden adoptar los volúmenes según su estado actual.

Tabla 3. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino		
	MOUNTABLE	NOTMOUNTABLE	COURIER
MOUNTABLE	N	S	S
NOTMOUNTABLE	N	N	S
COURIER	N	N	N
VAULT	N	N	N
VAULTRETRIEVE	N	N	N
COURIERRETRIEVE	N	N	N
ONSITERETRIEVE	N	N	N

Tabla 4. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino	
	VAULT	VAULTRETRIEVE
MOUNTABLE	S	N
NOTMOUNTABLE	S	N
COURIER	S	N
VAULT	N	N
VAULTRETRIEVE	N	N
COURIERRETRIEVE	N	N
ONSITERETRIEVE	N	N

Tabla 5. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino	
	COURIERRETRIEVE	ONSITERETRIEVE
MOUNTABLE	N	N
NOTMOUNTABLE	N	N
COURIER	N	N
VAULT	N	N
VAULTRETRIEVE	S	S

El estado actual del volumen	Estado de destino	
	COURIERRETRIEVE	ONSITERETRIEVE
COURIERRETRIEVE	N	S
ONSITERETRIEVE	N	N

Ejemplo: traspasar medios de recuperación ante siniestro desde el estado NOTMOUNTABLE

Traspasar medios de recuperación ante siniestro que se encuentran en estado NOTMOUNTABLE al estado COURIER y, a continuación, consultar los resultados.

```
move drmedia * wherestate=notmountable
tostate=courier
```

```
query actlog search="MOVE DRMEDIA"
```

```
08/11/1999 11:12:24 ANR0984I Proceso 10 para MOVE DRMEDIA
                    iniciado
                    en BACKGROUND a las 11:12:24.
08/11/1999 11:12:24 ANR0610I MOVE DRMEDIA iniciado por
                    HSIAO como
                    proceso 10.
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen TAPE0P ha pasado
                    del estado NOTMOUNTABLE al
                    estado COURIER.
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen TAPE1P ha pasado
                    del estado NOTMOUNTABLE al
                    estado COURIER.
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen DBTP02 ha pasado
                    del estado NOTMOUNTABLE al
                    estado COURIER.
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen DBTP01 ha
                    pasado
                    del estado NOTMOUNTABLE al
                    estado COURIER.
08/11/1999 11:12:25 ANR6682I El mandato MOVE DRMEDIA ha
                    finalizado 4 volúmenes
                    procesados.
08/11/1999 11:12:25 ANR0611I MOVE DRMEDIA iniciado por HSIAO
                    como
                    proceso 10 ha finalizado.
08/11/1999 11:12:25 ANR0985I Proceso 10 para MOVE DRMEDIA
                    ejecutándose
                    BACKGROUND ha procesado
                    4 elementos y ha tenido un estado
                    de
                    terminación de SUCCESS a las 11:12:25.
```

Ejemplo: traspasar medios de recuperación ante siniestro desde el estado MOUNTABLE

Traspasar medios de recuperación ante siniestro desde el estado MOUNTABLE al estado COURIER. Si el medio está en una biblioteca automatizada, MOVE DRMEDIA expulsa el medio antes de cambiar el estado.

```
move drmedia * wherestate=mountable tostate=courier wait=yes
```

```
ANR0984I Proceso 12 para MOVE DRMEDIA iniciado
                    en FOREGROUND a las 09:57:17.
ANR0609I MOVE DRMEDIA iniciado como proceso 12.
ANR0610I MOVE DRMEDIA iniciado por HSIAO como
                    proceso 12.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para
                    volumen TAPE01 de biblioteca LIB8MM iniciándose.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el
                    volumen TAPE01 de biblioteca LIB8MM se ha completado
                    correctamente.
ANR6683I MOVE DRMEDIA: El volumen TAPE01 ha pasado del
                    estado MOUNTABLE al estado COURIER.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para
                    volumen TAPE02 de biblioteca LIB8MM iniciándose.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el
                    volumen TAPE02 de biblioteca LIB8MM se ha completado
                    correctamente.
ANR6683I MOVE DRMEDIA: El volumen TAPE02 ha pasado del
```


estado MOUNTABLE al estado COURIER.
 ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para volumen DBTP05 de biblioteca LIB8MM iniciándose.
 ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el volumen DBTP05 de biblioteca LIB8MM se ha completado correctamente.
 ANR6683I MOVE DRMEDIA: El volumen DBTP05 ha pasado del estado MOUNTABLE al estado COURIER.
 ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para volumen DBTP04 de biblioteca LIB8MM iniciándose.
 ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el volumen DBTP04 de biblioteca LIB8MM se ha completado correctamente.
 ANR6683I MOVE DRMEDIA: El volumen DBTP04 ha pasado del estado MOUNTABLE al estado COURIER.
 ANR6682I Mandato MOVE DRMEDIA finalizado: 4 volúmenes procesados.
 ANR0611I MOVE DRMEDIA iniciado por HSIAO como el proceso 12 ha finalizado.
 ANR0985I Proceso 12 para MOVE DRMEDIA ejecutándose en FOREGROUND ha procesado 4 elementos con un estado de terminación de SUCCESS a las 10:12:25.

Ejemplo: traspasar medios de recuperación ante siniestro desde el estado VAULTRETRIEVE

Traspasar los medios de recuperación ante siniestro del estado VAULTRETRIEVE al estado ONSITERETRIEVE. Generar un mandato CHECKIN LIBVOLUME para cada volumen que se procesa correctamente y almacenar los mandatos en un archivo:

 Sistemas operativos AIX  Sistemas operativos Linux

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=/drm/move/exec.cmds
cmd="checkin libvol lib8mm &vol status=scratch"
```

 Sistemas operativos Windows

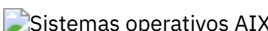
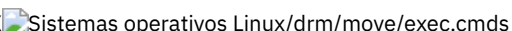
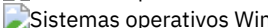
```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=c:\drm\move\exec.cmd
cmd="checkin libvol lib8mm &vol status=scratch"
```

Consultar los resultados:

```
query actlog search="MOVE DRMEDIA"

08/13/1999 09:12:24 ANR0984I Proceso 15 para MOVE DRMEDIA iniciado en
BACKGROUND a las 09:12:24.
08/13/1999 09:12:24 ANR0610I MOVE DRMEDIA iniciado por HSIAO como
proceso 15.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen CSTP01
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen CSTP02
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen DBTP10
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen DBTP11
se ha suprimido.
08/13/1999 09:12:27 ANR6682I El mandato MOVE DRMEDIA ha finalizado:
4 volúmenes
procesados.
08/13/1999 09:12:42 ANR0611I MOVE DRMEDIA iniciado por HSIAO como
proceso 15 ha finalizado.
08/13/1997 09:12:42 ANR0985I Proceso 15 para MOVE DRMEDIA
ejecutándose en
BACKGROUND ha procesado
4 elementos y ha tenido un estado
de terminación de SUCCESS a las
09:12:42.
```

Los mandatos para dar de alta los volúmenes también se han creado en el archivo especificado con el parámetro CMDFILENAME:

-  Sistemas operativos AIX  Sistemas operativos Linux/drm/move/exec.cmds
-  Sistemas operativos Windows c:\drm\move\exec.cmd

El archivo contiene estas líneas:

```


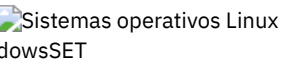
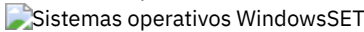

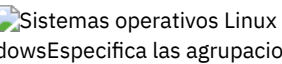

checkin libvol lib8mm CSTEP01 status=scratch
checkin libvol lib8mm CSTEP02 status=scratch
checkin libvol lib8mm DBTP10 status=scratch
checkin libvol lib8mm DBTP11 status=scratch

```

Consejo: Para procesar los mandatos CHECKIN LIBVOLUME, emita el mandato MACRO con el nombre de archivo como el nombre de macro.

Mandatos relacionados

Tabla 6. Mandatos relacionados con MOVE DRMEDIA

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
PREPARE	Crea un archivo de plan de recuperación.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY PROCESS	Muestra información sobre procesos subordinados.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMCOURIERNAME	Especifica el nombre del transportista del medio de recuperación ante siniestro.
SET DRMDBBACKUPEXPIREDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMVAULTNAME	Especifica el nombre de la cámara de seguridad donde está almacenado el medio DRM.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.
SET DRMFILEPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.
SET DRMNOTMOUNTABLENAME	Especifica el nombre de ubicación del medio DRM que se ha de enviar fuera del local.

MOVE GRPMEMBER (Mover un miembro de grupo de servidores)

Utilice este mandato para traspasar un miembro de un grupo de servidores a otro grupo de servidores. El mandato no se ejecutará si el miembro que se traspasa tiene el mismo nombre que uno de los miembros actuales del grupo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-MOVE GRPMEMber--nombre_miembro--grupo_origen--grupo_destino-><
```

Parámetros

nombre_miembro (Obligatorio)
Especifica el miembro (un servidor o un grupo de servidores) que se traspasa.
grupo_origen (Obligatorio)
Especifica el grupo de servidores al que está asociado actualmente el miembro.
grupo_destino (Obligatorio)
Especifica el nuevo grupo de servidores del miembro.

Ejemplo: traspasar un servidor a otro grupo de servidores

Traspasar el miembro PAYSON del grupo REGION1 al grupo REGION2.

```
move grpmember payson region1 region2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con MOVE GRPMEMBER

Mandato	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)

Utilice este mandato para gestionar agrupaciones de almacenamiento de desbordamiento. La base de datos hace el seguimiento de los medios que se traspasan utilizando este mandato..

Este mandato se aplica a los volúmenes de las agrupaciones de almacenamiento primarias y de copia gestionadas por una biblioteca automatizada (que puede ser externa). La biblioteca no tiene que estar llena. Se pueden procesar al mismo tiempo uno o más volúmenes de agrupaciones de almacenamiento de acceso secuencial.

Utilice el parámetro DAYS para identificar los volúmenes elegibles para ser trasladados. Utilice el parámetro OVERFLOW LOCATION para registrar la ubicación de almacenamiento de los medios traspasados.

Este mandato genera un proceso subordinado que puede visualizar utilizando el mandato QUERY PROCESS. Para cancelarlo, emita el mandato CANCEL PROCESS.

Para determinar si el mandato se ha ejecutado correctamente, emita el mandato QUERY ACTLOG o bien utilice la consola del servidor.

Los volúmenes que se trasladan mediante el mandato MOVE DRMEDIA para la recuperación fuera de local no se procesan mediante el mandato MOVE MEDIA.

entre 0 y 9999. El valor predeterminado es 0. Para calcular el número de días transcurridos se utiliza la fecha de la última grabación o la fecha de la última lectura de los volúmenes, la más reciente de las dos.

WHEREState

Especifica el estado actual de los volúmenes que se han de procesar. Este parámetro se utiliza para limitar el proceso a volúmenes que se encuentran en el estado especificado. Este parámetro es opcional. El valor predeterminado es MOUNTABLEINLIB.

Los valores posibles son:

MOUNTABLEInlib

Especifica que se ha de realizar el traslado de los volúmenes de agrupación de almacenamiento del estado MOUNTABLEINLIB al estado MOUNTABLENOTINLIB. Los volúmenes en estado MOUNTABLEINLIB contienen datos válidos y están en la biblioteca.

MOUNTABLENotinlib

Especifica que los volúmenes de agrupación de almacenamiento deben volver a cambiar del estado MOUNTABLENOTINLIB al estado MOUNTABLEINLIB. Los volúmenes en estado MOUNTABLENOTINLIB pueden contener datos válidos y están en la ubicación de desbordamiento.

- Para los volúmenes reutilizables vacíos, el mandato MOVE MEDIA suprime los registros de volúmenes para que éstos puedan volver a utilizarse.
- Para los volúmenes privados, el mandato MOVE MEDIA restablece la ubicación del volumen en un valor en blanco, cambia el estado del volumen a CHECKIN y cambia la fecha de la última actualización a la fecha actual.
- Para los volúmenes reutilizables con datos, el mandato MOVE MEDIA restablece la ubicación del volumen en un valor en blanco, cambia el estado del volumen a CHECKIN y cambia la fecha de la última actualización a la fecha actual.

Atención: Los volúmenes que están en el estado CHECKIN pueden contener datos válidos y no es necesario darlos de alta en la biblioteca.

WHERESTATUS

Especifica que el proceso de traslado debe ser restringido por el estado de volumen. Este parámetro es opcional. Puede especificar varios estados en una lista si separa cada uno con una coma sin dejar espacios intercalados. Si no especifica este parámetro, los volúmenes traspasados del estado MOUNTABLEINLIB al estado MOUNTABLENOTINLIB están restringidos a sólo los volúmenes llenos, y los volúmenes traspasados del estado MOUNTABLENOTINLIB al estado MOUNTABLEINLIB están restringidos a sólo los volúmenes vacíos.

Los valores posibles son:

FULL

Se traspasan los volúmenes con el estado FULL.

FILLing

Se traspasan los volúmenes con el estado FILLING.

EMPTy

Se traspasan los volúmenes con el estado EMPTY.

ACCess

Especifica la forma en que los usuarios y los procesos del sistema acceden a los archivos del volumen de agrupación de almacenamiento que se traslada desde una biblioteca automatizada y se almacena en una ubicación de desbordamiento mediante el mandato MOVE MEDIA. Este parámetro es opcional. Si no especifica este parámetro, el traslado de los volúmenes desde el estado MOUNTABLEINLIB hasta el proceso MOUNTABLENOTINLIB actualiza la modalidad de acceso de los volúmenes a READONLY, y el traslado de los volúmenes desde el estado MOUNTABLENOTINLIB hasta el proceso MOUNTABLEINLIB actualiza la modalidad de acceso de los volúmenes a READWRITE.

Los valores posibles son:

READWrite

Especifica que los usuarios y los procesos del sistema pueden leer y grabar en archivos almacenados en el volumen que está en la ubicación de desbordamiento. Si se especifica este valor, IBM Spectrum Protect solicita que se dé de alta el volumen en la biblioteca cuando se necesita el volumen para una operación de lectura o grabación.

READOnly

Especifica que los usuarios y los procesos del sistema pueden leer pero no grabar en los archivos que están almacenados en el volumen que está en la ubicación de desbordamiento. El servidor sólo solicita que se dé de alta el volumen en la biblioteca cuando el volumen se necesita para una operación de lectura.

OVFLocation

Especifica la ubicación de desbordamiento que es el destino de los volúmenes que están procesándose. La longitud máxima del nombre de ubicación son 255 caracteres. La información de nombre de ubicación debe estar delimitada con comillas si contiene caracteres en blanco. Si no especifica una ubicación de desbordamiento y la agrupación de almacenamiento tampoco tiene

ninguna ubicación de desbordamiento identificada, el servidor cambia la ubicación del volumen expulsado por una serie nula ("").

REMove

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles son YES, BULK y NO. El valor predeterminado es BULK. La respuesta del servidor a cada una de estas opciones y los valores predeterminados se describen en las siguientes tablas.

Bibliotecas 349X: En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas 349X.

Tabla 1. Cómo responde el servidor en las bibliotecas 349X

REMOVE=YES	REMOVE=BULK	REMOVE=NO
El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.	El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.	El gestor de biblioteca 3494 no expulsa el volumen. El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

Bibliotecas SCSI: La tabla siguiente muestra cómo responde el servidor ante las opciones YES, BULK y NO en las bibliotecas SCSI.

Tabla 2. Cómo responde el servidor en las bibliotecas SCSI

Si una biblioteca...	Y REMOVE=YES...	Y REMOVE=BULK...	Y REMOVE=NO
No tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Tiene puertos de entrada/salida y un puerto de entrada/salida está disponible	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje. El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Tiene puertos de entrada/salida, pero no hay puertos disponibles	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor espera que un puerto de entrada/salida se haga disponible.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje. El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.

Bibliotecas ACSLS: En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas ACSLS.

Tabla 3. Cómo responde el servidor en las bibliotecas ACSLS

REMOVE=YES o REMOVE=BULK	REMOVE=NO
--------------------------	-----------

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho en la estación de E/S que convenga.	El servidor no expulsa el cartucho.
El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.	El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.
Mientras tiene lugar el traspaso de volúmenes del estado MOUNTABLE cuando se ha especificado REMOVE=YES, el mandato MOVE MEDIA utiliza más de una ranura del CAP para una biblioteca StorageTek que dispone de software ACSLS.	



Bibliotecas externas: En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas externas.


Tabla 4. Cómo responde el servidor en las bibliotecas externas

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho en la estación de E/S que convenga. El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.	El servidor no expulsa el cartucho.
	El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

CMd

Especifica la creación de mandatos ejecutables. Este parámetro es opcional. La especificación de mandatos ejecutables se ha de encerrar entre comillas. La longitud máxima de la especificación del mandato ejecutable es de 255 caracteres. Para cada volumen que procese correctamente el mandato MOVE MEDIA, el servidor graba los mandatos asociados en un archivo. Especifique el nombre de archivo con el parámetro CMDFILENAME.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica el nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie exec.cmds.media al directorio del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no especifica el nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie exec.cmd.media al directorio del servidor de IBM Spectrum Protect.

Si la longitud del mandato escrito en el archivo sobrepasa los 255 caracteres, se divide en varias líneas y se añade un carácter de continuación, +, a todas menos a la última línea del mandato. Puede que deba alterar el carácter de continuación en función de los requisitos del producto que ejecuta los mandatos.

Si no especifica CMD, el mandato MOVE MEDIA no generará ningún mandato ejecutable.

serie

Especifica la serie para crear un mandato ejecutable. Puede especificar cualquier texto de formato libre para la serie. Encierre toda la serie entre comillas. Por ejemplo, la siguiente es una especificación válida de un mandato ejecutable:

```
CMD="UPDATE VOLUME &VOL"
```

La siguiente es una especificación no válida de un mandato ejecutable:

```
CMD=""UPDATE VOLUME" &VOL"
```

sustitución

Especifica una variable para la que desea que el mandato sustituya un valor. Las posibles variables de sustitución son:

&VOL

Sustituye el nombre de volumen por &VOL. Puede especificar caracteres en minúsculas, &vol. No debe especificar ni espacios ni blancos entre el signo & y VOL. Si existen espacios o blancos entre el ampersand y VOL, el mandato MOVE MEDIA los trata como series y no se establece ninguna sustitución. Si no se especifica &VOL, no se establecerá ningún nombre de volumen en el mandato ejecutable.

&LOC

Sustituye que el volumen por &LOC. Puede especificar caracteres en minúsculas, &loc. No debe especificar ni espacios ni blancos entre el signo & y LOC. Si existen espacios o blancos entre el ampersand y LOC, el mandato MOVE MEDIA los trata como series y no se establece ninguna sustitución. Si no se especifica &LOC, no se establecerá ningún nombre de ubicación en el mandato ejecutable.

&VOLDSN



Sustituye el nombre de archivo del volumen por &VOLDSN. Un ejemplo de un nombre de archivo de volumen de cinta de agrupación de almacenamiento que utiliza el prefijo predeterminado ADSM es ADSM.BFS. Si no se especifica &VOLDSN, no se establecerá ningún nombre de archivo de volumen en el mandato ejecutable.


&NL

Sustituye un nuevo carácter de línea por &NL. Cuando se especifica &NL, el mandato MOVE MEDIA subdivide el mandato en la posición en la que se encuentra &NL y no añade ningún carácter de continuación. El usuario es el responsable de especificar el carácter de continuación correcto antes de &NL, si es necesario. El usuario también es el responsable de la longitud de la línea escrita. Si no se especifica &NL y la longitud de la línea de mandatos sobrepasa los 255 caracteres, la línea de mandatos se dividirá en varias líneas y se añadirá un carácter de continuación, +, a todas menos a la última línea del mandato.

CMDFilename

Especifica el nombre completo de vía de acceso de un archivo que contiene los mandatos que se han especificado con CMD. Este parámetro es opcional. La longitud máxima del nombre de archivo es de 1279 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica un nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie `exec.cmds.media` al directorio del servidor de IBM Spectrum Protect. El directorio del servidor es el directorio de trabajo actual del proceso servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no especifica un nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie `exec.cmd.media` al directorio del servidor de IBM Spectrum Protect. El directorio del servidor es el directorio de trabajo actual del proceso servidor de IBM Spectrum Protect.

El mandato MOVE MEDIA asigna automáticamente el nombre de archivo que se ha especificado o generado. Si existe el nombre de archivo, puede utilizar el parámetro APPEND=YES para agregarlo al archivo. De lo contrario, el archivo quedará sobregabado. Si un archivo se ha sobregabado por accidente y debe ejecutar los mandatos que contenía el archivo, emita el mandato QUERY MEDIA para volver a crear los mandatos ejecutables para los volúmenes deseados. Si el mandato MOVE MEDIA no se ejecuta correctamente después de haberse asignado el archivo de mandatos, el archivo no se suprimirá.

APPend

Especifica que se graba al principio o al final de los datos del archivo de mandatos. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se han de escribir datos desde el principio del archivo de mandatos. Si el archivo de mandatos ya existe, se sobregabará el contenido.

Yes

Especifica que se agrega el archivo de mandatos grabando al final de los datos del archivo de mandatos.

CHECKLabel

Especifica si el servidor lee las etiquetas de los volúmenes de los medios secuenciales. Con los dispositivos SCSI, puede suprimir la comprobación de etiquetas si establece CHECKLabel en NO. Este parámetro no es aplicable a las bibliotecas 349X. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que el servidor intenta leer la etiqueta del medio. Leer la etiqueta del medio verifica que se está dando de baja el volumen correcto.

No

Especifica que el servidor no intenta leer la etiqueta del medio. De este modo aumenta el rendimiento ya que no se produce el proceso de lectura.

CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

x

El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.

y

El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.

z

El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

Ejemplo: trasladar todos los volúmenes fuera de la biblioteca


Trasladar fuera de la biblioteca todos los volúmenes completos que estén en la agrupación de almacenamiento primaria secuencial ARCHIVE.

```
move media * stgpool=archive
```

Ejemplo: generar los mandatos para dar de alta

Generar los mandatos CHECKIN LIBVOLUME para los volúmenes llenos y parcialmente llenos que están en la agrupación de almacenamiento primaria ONSITE.ARCHIVE y almacenados en la ubicación de desbordamiento, room2948/bldg31.




 Sistemas operativos AIX  Sistemas operativos Linux MOVE MEDIA crea los mandatos ejecutables en /tsm/move/media/checkin.vols

 Sistemas operativos Windows MOVE MEDIA crea los mandatos ejecutables en c:\tsm\move\media\checkin.vols

```
move media * stgpool=onsite.archive
wherestate=mountablenotinlib wherestatus=full,filling
ovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

```
checkin libvolume lib3494 TAPE04 status=private
checkin libvolume lib3494 TAPE13 status=private
checkin libvolume lib3494 TAPE14 status=private
```

Consejo: Ejecute el mandato CHECKIN LIBVOLUME emitiendo el mandato MACRO con la información siguiente como nombre de macro:

-  Sistemas operativos AIX  Sistemas operativos Linux /tsm/move/media/checkin.vols
-  Sistemas operativos Windows c:\tsm\move\media\checkin.vols

Mandatos relacionados

Tabla 5. Mandatos relacionados con MOVE MEDIA

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY MEDIA	Muestra información acerca de los volúmenes de agrupaciones de almacenamiento que se ha trasladado mediante el mandato MOVE MEDIA.
QUERY PROCESS	Muestra información sobre procesos subordinados.

MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)

Utilice este mandato para trasladar datos que se encuentran en una agrupación de almacenamiento de acceso secuencial. Puede trasladar datos para uno o más nodos, o para un grupo de nodos asignados con espacios de archivos seleccionados. También puede trasladar espacios de archivos seleccionados para un solo nodo. Los datos se pueden encontrar en una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia o una agrupación de datos activos.

Este mandato es útil para reducir el número de montajes de volúmenes durante las operaciones de restauración o de recuperación del cliente, pues consolida los datos para un nodo específico dentro de una agrupación de almacenamiento, o bien para traspasar los datos a otra agrupación de almacenamiento. Por ejemplo, puede utilizar este mandato para traspasar datos a una agrupación de almacenamiento de acceso aleatorio como preparación para el proceso de restauración del cliente.

Asegúrese de que la modalidad de acceso de los volúmenes desde los que está trasladando los datos del nodo sea de lectura y grabación o de lectura y que la modalidad de acceso de los volúmenes a los que está trasladando los datos del nodo se haya establecido para lectura/grabación. Esta operación no trasladará los datos de los volúmenes cuyas modalidades de acceso sean fuera del local, no disponible o destruido.

El mandato MOVE NODEDATA adopta dos formas, en función de si traspasa datos sólo para los espacios de archivo seleccionados. La sintaxis y los parámetros de cada formato se definen por separado.

Restricción: No puede trasladar datos de nodo a o desde una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Tabla 1. Mandatos relacionados con MOVE NODEDATA

Mandato	Descripción
---------	-------------

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.

- MOVE NODEDATA (Trasladar datos de los espacios de archivos para uno o varios nodos o un grupo de proximidad)
Utilice este mandato para mover los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.
- MOVE NODEDATA (Traspasar datos desde espacios de archivos seleccionados de un único nodo)
Utilice este mandato para traspasar datos para espacios de archivos seleccionados que pertenecen al mismo nodo.

MOVE NODEDATA (Trasladar datos de los espacios de archivos para uno o varios nodos o un grupo de proximidad)

Utilice este mandato para mover los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento origen. Si su autorización tiene privilegio de almacenamiento con restricciones y tiene previsto traspasar datos a otra agrupación de almacenamiento, debe tener la autorización adecuada para la agrupación de almacenamiento de destino.

Sintaxis

```

      .,-----
      v         |
>>>MOVE NODEdata--+-+---nombre_nodo-+-+-----+----->
                    '-COLLOGGroup--+-+---nombre_grupo-+'

```



```

>--FROMstgpool---nombre_agrupación_origen----->
>+-----+----->
' -Tostgpool---nombre_agrupación_destino-'
. -Type---ANY-----
>+-----+----->
' -Type---+ANY-----+ '
      +-Backup-----+
      +-ARChive-----+
      '-SPacemanaged-'

. -MAXPRocess---1----- . -Wait---No-----
>+-----+-----+----->
' -MAXPRocess---núm_procesos-' ' -Wait---+No--+-'
                                     '-Yes-'

(1)
. -RECONStruct---No o Yes-----
>+-----+-----><
' -RECONStruct---+No--+-----+ '
      '-Yes-'

```

Notas:

1. El valor predeterminado es NO si la agrupación de almacenamiento de origen o de destino es de acceso aleatorio. El valor predeterminado es YES si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial.

Parámetros

nombre_nodo (Necesario, a menos que se especifique el parámetro COLLOGROUP)

Especifica el nombre de nodo relacionado con los datos que se traspasan con este mandato. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

COLLOGroup (Necesario, a menos que se haya especificado el parámetro nombre_nodo)

Especifica el nombre del grupo de proximidad cuyos datos que deben traspasarse. Se traspasan los datos de todos los nodos y espacios de archivos pertenecientes al grupo de proximidad.

FROMstgpool (Obligatorio)

Especifica el nombre de una agrupación de almacenamiento de acceso secuencial que contiene datos que deben traspasarse. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK.

Tostgpool

Especifica el nombre de una agrupación de almacenamiento a la que se traspasan los datos. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK. Este parámetro es opcional y no se aplica si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia o una agrupación de datos activos. Es decir, si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia, el destino debe ser la misma agrupación de almacenamiento de copia. De forma parecida, si la agrupación de almacenamiento origen es una agrupación de datos activos, el destino debe ser la misma agrupación de datos activos. Si no se especifica ningún valor, se traspasan los datos a otros volúmenes de la agrupación de almacenamiento origen.

Importante: Si va a traspasar datos en la misma agrupación de almacenamiento, debe haber volúmenes disponibles que no contengan los datos del nodo que va a traspasar. Es decir, el servidor no puede utilizar volúmenes que contengan los datos que se van a traspasar como volúmenes de destino.

Type

Especifica el tipo de archivos que se traspasará. Este parámetro es opcional. El valor predeterminado es ANY. Si la agrupación de almacenamiento origen es una agrupación de datos activos, los únicos valores válidos son ANY y BACKUP. Sin embargo, si TYPE=ANY sólo se trasladan las versiones activas de los datos de copia de seguridad. Especifique uno de los siguientes valores:

ANY

Especifica que se traspasan todos los tipos de archivos.

Backup

Especifica que se traspasan archivos de copia de seguridad.

ARChive

Especifica que se traspasan copias archivadas. Este valor no es válido para las agrupaciones de datos activos.

SPacemanaged

Especifica que se trasladan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management). Este valor no es válido para las agrupaciones de datos activos.

MAXPRocess

Especifica el número máximo de procesos paralelos que se utilizará para traspasar datos. Este parámetro es opcional. Puede especificar un valor entre 1 y 999, ambos incluidos. El valor predeterminado es 1. Si se aumenta el número de procesos

paralelos, normalmente se mejora el rendimiento.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo secuencial no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otra actividad del sistema de IBM Spectrum Protect. Los puntos de montaje y unidades también dependen de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en el traslado. Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento y, si el tipo de dispositivo no es FILE, también necesita una unidad.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Especifique uno de los siguientes valores:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano, es posible que ya se hayan traspasado algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

RECONStruct

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de una agregación. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO. El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento.

Puede especificar uno de los siguientes valores:

No

Especifica que la reconstrucción de agregaciones de archivos no se realiza durante la operación de traspaso.

Yes

Especifica que la reconstrucción de agregaciones de archivos no se realiza durante la operación de traspaso. Solo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

Traspasar datos de un nodo específico desde una agrupación de almacenamiento de cinta hasta una agrupación de almacenamiento de disco

Traspasar todos los datos que pertenecen al nodo MARY almacenado en la agrupación de almacenamiento TAPEPOOL. Los datos deben traspasarse a la agrupación de almacenamiento de disco BACKUPPOOL.

```
move nodedata mary
  fromstgpool=tapepool tostgpool=backuppool
```

Traspasar datos para un grupo de proximidad de nodo desde una agrupación de almacenamiento a otra

Traspasar todos los datos para el grupo de proximidad de nodo NODEGROUP1 desde la agrupación de almacenamiento SOURCEPOOL a la agrupación de almacenamiento TARGETPOOL.

```
move nodedata collocgroup=nodegroup1 fromstgpool=sourcespool tostgpool=targetpool
```

Traspasar datos para un grupo de proximidad de espacio de archivos desde una agrupación de almacenamiento a otra

Traspasar todos los datos para el grupo de proximidad de espacio de archivos FSGROUP1 desde la agrupación de almacenamiento SOURCEPOOL2 a la agrupación de almacenamiento TARGETPOOL2.

```
move nodedata collocgroup=fsgroup1 fromstgpool=sourcespool2 tostgpool=targetpool2
```

MOVE NODEDATA (Traspasar datos desde espacios de archivos seleccionados de un único nodo)

Utilice este mandato para traspasar datos para espacios de archivos seleccionados que pertenecen al mismo nodo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento origen. Si tiene privilegio de almacenamiento con restricciones y tiene previsto traspasar datos a otra agrupación de almacenamiento, debe tener la autorización adecuada para la agrupación de almacenamiento destino.

Sintaxis

```
>>-MOVE NODEdata--nombre_nodo----->
>--FROMstgpool---nombre_agrupación_origen----->
>+-----+----->
  '-Tostgpool---nombre_agrupación_destino-'
>+-----+----->
  |           .-,------. |
  |           v             | |
  '-Filespace---nombre_espacio_archivos-+-'
>+-----+----->
  |           .-,------. |
  |           v             | |
  '-UNIFILESpace---nombre_espacio_archivos_unicode-+-'
>+-----+----->
  |           .-,------. |
  |           v             | |
  '-FSID---identificador_espacio_archivos-+-'
  .-Type---ANY-----
>+-----+----->
  '-Type---ANY-----+'
          +-Backup-----+
          +-ARchive-----+
          '-SPacemanaged-'
  .-MAXProcess---1----- .-Wait---No-----
>+-----+----->
  '-MAXProcess---núm_procesos-' '-Wait---+-No-+-'
                                   '-Yes-'
(1)
  .-RECONstruct---No o Yes-----
>+-----+----->
  '-RECONstruct---+-No-+-'
          '-Yes-'
```

Notas:

1. El valor predeterminado es NO si la agrupación de almacenamiento de origen o de destino es de acceso aleatorio. El valor predeterminado es YES si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre de nodo relacionado con los datos que se traspasan en este mandato. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

FROMstgpool (Obligatorio)

Especifica el nombre de una agrupación de almacenamiento de acceso secuencial que contiene datos que deben traspasarse. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK.

TOstgpool

Especifica el nombre de una agrupación de almacenamiento a la que se traspasarán los datos. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK. Este parámetro es opcional y no se aplica si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia o una agrupación de datos activos. Es decir, si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia, el destino debe ser la misma agrupación de almacenamiento de copia. De forma parecida, si la agrupación de almacenamiento origen es una agrupación de datos activos, el destino debe ser la misma agrupación de datos activos. Si no se especifica ningún valor, se traspasan los datos a otros volúmenes de la agrupación de almacenamiento origen.

Importante: Si va a traspasar datos en la misma agrupación de almacenamiento, deberá haber volúmenes disponibles que no contengan los datos del nodo que va a traspasar. Es decir, el servidor no puede utilizar volúmenes que contengan los datos que se van a traspasar como volúmenes de destino.

FILEspace

Especifica el nombre del espacio de archivos no Unicode que contiene los datos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional. Si no especifica un valor para este parámetro ni valores para UNIFILESPACE, FSID o ambos, no se traspasarán los espacios de archivos que no son Unicode.

UNIFILESpace

Especifica el nombre del espacio de archivos Unicode que contiene los datos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional. Si no especifica un valor para este parámetro ni valores para FILESPACE, FSID o ambos, no se traspasarán los espacios de archivos que no son Unicode.

FSID

Especifica los identificadores de espacios de archivos (FSID) de los espacios de archivos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Type

Especifica el tipo de archivos que se traspasará. Este parámetro es opcional. El valor predeterminado es ANY. Si la agrupación de almacenamiento origen es una agrupación de datos activos, los únicos valores válidos son ANY y BACKUP. Sin embargo, si TYPE=ANY sólo se trasladan las versiones activas de los datos de copia de seguridad. Los valores posibles son:

ANY

Especifica que se traspasan todos los tipos de archivos.

Backup

Especifica que se traspasan archivos de copia de seguridad.

ARchive

Especifica que se traspasan copias archivadas. Este valor no es válido para las agrupaciones de datos activos.

SPacemanaged

Especifica que se trasladan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management). Este valor no es válido para las agrupaciones de datos activos.

MAXPRocess

Especifica el número máximo de procesos paralelos que se utilizará para traspasar datos. Este parámetro es opcional. Puede especificar un valor entre 1 y 999, ambos incluidos. El valor predeterminado es 1. Si se aumenta el número de procesos paralelos se mejorará el rendimiento.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo secuencial no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otra actividad del sistema de IBM Spectrum Protect y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en el traslado. Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento y, si el tipo de dispositivo no es FILE, también necesita una unidad.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano, es posible que ya se hayan traspasado algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

RECONSTRUCT

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de un conjunto. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO. El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento. Los valores posibles son:

No

Especifica que la reconstrucción de agregaciones de archivos no se realizará durante la operación de traspaso.

Yes

Especifica que la reconstrucción de agregaciones de archivos se realizará durante la operación de traspaso. Sólo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

Ejemplo: trasladar datos no Unicode y Unicode de un nodo

Trasladar datos para el nodo TOM en la agrupación de almacenamiento TAPEPOOL. Limitar el traslado de datos a archivos en espacios de archivos no Unicode y en espacios de archivos Unicode, \\jane\d\$. Los datos deben traspasarse a la agrupación de almacenamiento de disco BACKUPPOOL.

```
move nodedata tom
  fromstgpool=tapepool tostgpool=backuppool
  filespace=* unifilespace=\\jane\d$
```

Ejemplo: trasladar datos de nodo desde agrupaciones de almacenamiento de cinta hasta una agrupación de almacenamiento de disco

Trasladar todos los datos del nodo SARAH, desde todas las agrupaciones de almacenamiento primarias de acceso secuencial (en este ejemplo, TAPEPOOL*) a DISKPOOL. Para obtener una lista de agrupaciones de almacenamiento que contienen datos para el nodo SARAH, emita uno de los mandatos siguientes: QUERY OCCUPANCY o SELECT:

```
query occupancy sarah

SELECT * from OCCUPANCY where node_name='sarah'
```

Atención: Para este ejemplo, se da por supuesto que los resultados son TAPEPOOL1, TAPEPOOL4 y TAPEPOOL5.

```
move nodedata sarah
  fromstgpool=tapepool1 tostgpool=DISKPOOL
```

```
move nodedata sarah
  fromstgpool=tapepool4 tostgpool=DISKPOOL
```

```
move nodedata sarah
  fromstgpool=tapepool15 tostgpool=DISKPOOL
```

Ejemplo: trasladar espacios de archivos no Unicode y Unicode de un nodo

El siguiente es un ejemplo de cómo trasladar a un nodo espacios de archivos de Unicode y que no sean de Unicode. Para el nodo NOAH, trasladar el espacio de archivos no Unicode \\servtuc\d\$ y el espacio de archivos Unicode \\tmserv1\e\$ que tiene el ID de espacio de archivos 2 desde la agrupación de almacenamiento de acceso secuencial TAPEPOOL hasta la agrupación de almacenamiento de acceso aleatorio DISKPOOL.

```
move nodedata noah
  fromstgpool=tapepool tostgpool=diskpool
  filespace=\\tmserv1\d$ fsid=2
```

NOTIFY SUBSCRIBERS (Notificar a servidores gestionados que actualicen los perfiles)

Utilice este mandato en un gestor de configuración para notificar a uno o varios servidores gestionados que soliciten que su información de configuración se renueve inmediatamente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-NOTIfy SUBSCRIBers--+-PROFIle-----*-----+-----><
|               .,-----+-----+-----|
|               v         |               |
|'-PROFIle-----nombre_perfil-+-'
```

Parámetros

PROFIle (Obligatorio)

Especifica el nombre del perfil. Se notifican los servidores gestionados que se suscriben al perfil. Puede utilizar caracteres comodín para especificar varios perfiles. Para especificar varios perfiles, debe separarlos con comas y sin espacios intercalados. El valor predeterminado es notificar a todos los suscriptores.

Ejemplo: notificar a los servidores gestionados que han de actualizarse los perfiles

Notificar a todos los servidores gestionados suscritos a un perfil denominado DELTA que han de solicitar información de configuración actualizada.

```
notify subscribers profile=delta
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con NOTIFY SUBSCRIBERS

Mandato	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.

Mandato	Descripción
SET CONFIGREFRESH	Especifica un intervalo de tiempo para que los servidores gestionados entren en contacto con los gestores de configuración.




PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca)

Utilice este mandato para definir o suprimir todas las unidades y sus rutas para una única biblioteca en un paso.

Este mandato puede utilizarse cuando se configura un entorno de biblioteca o se modifica una configuración de hardware existente que requiere cambios en muchas definiciones de unidad. Después de definir una biblioteca, emita PERFORM LIBACTION para definir unidades y sus rutas para la biblioteca. También puede suprimir todas las unidades y rutas de una biblioteca emitiendo el mandato con ACTION=DELETE.

Este mandato sólo es válido para los tipos de biblioteca SCSI y VTL. Para utilizar este mandato con ACTION=DEFINE, la opción SANDISCOVERY debe estar soportada y habilitada.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-PERForm LIBACTIon--nombre_biblioteca----->
>---ACTIon-----+DEFine--| A |----->
      +-DELeTe-----+
      +-RESet--| B |--+
      '-QUIesce-----'

      .-PREView----No-----.
>+-----+-----+-----+-----><
  '-SOURCe----nombre_origen-' '-PREView----+Yes+-'
                               '-No--'

A (DEFine)
|-----+----->
  '-DEVIce----nombre_dispositivo_biblioteca-'

  .-PREFix----nombre_biblioteca----.
>+-----+-----|
  '-PREFix----nombre_prefijo_unidad-'

B (RESet)

      .-DRIVEsonly----No-----.
|---ACTIon-----RESet-----+-----|
      '-DRIVEsonly----+Yes+-'
                          '-No--'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se va a definir o suprimir. La longitud máxima de este nombre es de 30 caracteres, a menos que emita PERFORM LIBACTION con ACTION=DEFINE y utilice el valor PREFIX predeterminado. En este caso, la longitud máxima del nombre es de 25 caracteres.

ACTION

Especifica la acción para el mandato PERFORM LIBACTION. Los valores posibles son:

DEFine

Especifica que las unidades y sus rutas están definidas para la biblioteca especificada. El descubrimiento SAN debe estar activado antes de especificar este valor de parámetro.

DELete

Especifica que las unidades y sus rutas se han suprimido para la biblioteca especificada.

RESet

Especifica que las unidades y sus rutas se han actualizado en línea para la biblioteca especificada.

DRIVEsonly

Especifica que sólo las unidades se actualizan en línea para la biblioteca especificada.

Los valores posibles son:

No

Especifica que las unidades y rutas se actualizan en línea.

Yes

Especifica que sólo las unidades se actualizan en línea.

QUIesce

Especifica que las unidades se actualizan fuera de línea.

DEVIce

Especifica el nombre de dispositivo de biblioteca que se utiliza cuando se definen rutas si no se ha definido todavía una ruta a la biblioteca. Si se ha definido una ruta, el parámetro DEVICE se ignora. La longitud máxima de este valor es de 64 caracteres. Este parámetro es opcional.

PREFix

Especifica el prefijo que se utiliza para todas las definiciones de unidad. Por ejemplo, un valor de PREFIX *DR* crea las unidades *DRO*, *DR1*, *DR2*, para tantas unidades como se creen. Si no se especifica un valor para el parámetro PREFIX, se utiliza el nombre de biblioteca como el prefijo de las definiciones de unidad. La longitud máxima de este valor es de 25 caracteres.

SOURCe

Especifica el nombre del servidor de origen que se utilizará cuando se definan o supriman definiciones de rutas de unidad en un cliente de biblioteca o en un cliente sin LAN. Utilice este parámetro sólo si las unidades de la biblioteca están configuradas para el servidor local. Si no se especifica ningún valor para el parámetro SOURCE, se utiliza el nombre de servidor local, que es el valor predeterminado. La longitud máxima del nombre de origen es de 64 caracteres.

Si especifica el parámetro SOURCE, puede realizar RESET sólo de las rutas de los valores SOURCE especificados. El parámetro SOURCE no es compatible con opciones RESET DRIVESONLY=YES o QUIESCE.

Si se especifica un nombre de origen distinto del nombre de servidor local con ACTION=DEFINE, las definiciones de ruta de unidad se definen con el valor de señal UNDISCOVERED. A continuación, los clientes de biblioteca que dan soporte al descubrimiento SAN actualizan dinámicamente las definiciones de ruta la primera vez que se monta la unidad.

PREView

Especifica la salida de todos los mandatos que se procesan para PERFORM LIBACTION antes de emitir el mandato. El parámetro PREVIEW no es compatible con el parámetro DEVICE. Si está emitiendo el mandato PERFORM LIBACTION para definir una biblioteca, no puede especificar a la vez el parámetro PREVIEW y DEVICE.

Los valores posibles son:

No

Especifica que no se muestra una vista previa de los mandatos emitidos para PERFORM LIBACTION.

Yes

Especifica que se muestra una vista previa de los mandatos emitidos para PERFORM LIBACTION.

Ejemplo: definir una biblioteca compartida

Supongamos que está trabajando en una SAN y que ha configurado un gestor de bibliotecas denominado LIBMGR1. Ahora, define una biblioteca que se denomina SHAREDTSM para un servidor cliente de biblioteca denominado LIBCL1.

Emita DEFINE LIBRARY desde el servidor cliente de biblioteca, LIBCL1:

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

A continuación, emita PERFORM LIBACTION desde el gestor de biblioteca, LIBMGR1, para definir las vías de acceso de unidad para el cliente de biblioteca:

```
perform libaction sharedtsm action=define source=libcl1
```



Nota: La opción SANDISCOVERY debe estar soportada y habilitada en el servidor de cliente de biblioteca.

Ejemplo: definir una biblioteca con cuatro unidades

Defina una biblioteca SCSI llamada KONA:

```
define library kona libtype=scsi
```

A continuación, emita el mandato PERFORM LIBACTION para definir las unidades y las rutas para la biblioteca:

 Sistemas operativos AIX

```
perform libaction kona action=define device=/dev/lb3  
prefix=dr
```

A continuación, el servidor ejecuta los siguientes mandatos:

```
define path server1 kona srct=server destt=library  
device=/dev/lb3  
define drive kona dr0  
define path server1 dr0 srct=server destt=drive library=kona  
device=/dev/mt1  
define drive kona dr1  
define path server1 dr1 srct=server destt=drive library=kona  
device=/dev/mt2  
define drive kona dr2  
define path server1 dr2 srct=server destt=drive library=kona  
device=/dev/mt3  
define drive kona dr3  
define path server1 dr3 srct=server destt=drive library=kona  
device=/dev/mt4
```

 Sistemas operativos Linux

```
perform libaction kona action=define device=/dev/tmsmcsi/lb3  
prefix=dr
```

A continuación, el servidor ejecuta los siguientes mandatos:

```
define path server1 kona srct=server destt=library  
device=/dev/tmsmcsi/lb3  
define drive kona dr0  
define path server1 dr0 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt1  
define drive kona dr1  
define path server1 dr1 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt2  
define drive kona dr2  
define path server1 dr2 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt3  
define drive kona dr3  
define path server1 dr3 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt4
```

 Sistemas operativos Windows

```
perform libaction kona action=define device=lb0.0.0.2  
prefix=dr
```

A continuación, el servidor ejecuta los siguientes mandatos:

```
define path server1 kona srct=server destt=library  
device=lb0.0.0.2  
define drive kona dr0  
define path server1 dr0 srct=server destt=drive library=kona  
device=mt0.1.0.2  
define drive kona dr1  
define path server1 dr1 srct=server destt=drive library=kona  
device=mt0.2.0.2  
define drive kona dr2  
define path server1 dr2 srct=server destt=drive library=kona  
device=mt0.3.0.2  
define drive kona dr3  
define path server1 dr3 srct=server destt=drive library=kona  
device=mt0.4.0.2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con PERFORM LIBACTION

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE PATH	Cambia los atributos asociados con una ruta.

PING SERVER (Comprobar la conexión entre servidores)

Utilice este mandato para comprobar la conexión entre el servidor local y un servidor remoto.

Importante: El nombre y la contraseña del administrador que emite este mandato también deben estar definidos en el servidor remoto. Si el servidor remoto está en el nivel actual, las credenciales del servidor se verifican automáticamente cuando se ejecuta el mandato PING SERVER. Si el servidor remoto no está en el nivel actual, las credenciales del servidor no se verifican.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>>-PING SERVER--nombre_servidor-----<<<
```

Parámetros

nombre_servidor (Obligatorio)
Especifica el nombre del servidor remoto.

Ejemplo: comprobar la conexión con un servidor

Comprobar la conexión con el servidor FRED.

```
ping server fred
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con PING SERVER

Mandato	Descripción
---------	-------------

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY SERVER	Muestra información sobre servidores.

PREPARE (crear un archivo de plan de recuperación)

Utilice este mandato para crear un archivo de plan de recuperación, que contiene la información necesaria para recuperar un servidor de IBM Spectrum Protect. El archivo del plan de recuperación se puede almacenar en un sistema de archivos que sea accesible para el servidor de origen o en un servidor de destino.

Puede utilizar el mandato QUERY ACTLOG para determinar si el mandato PREPARE se ha ejecutado correctamente.

También puede ver esta información desde la consola del servidor o, si el parámetro WAIT es YES, en una sesión de cliente de administración.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.-Source----DBBackup-----
>>-Prepare----->
      '-Source----+DBBackup---+'
              '-DBSnapshot-'

>----->
      '-DEVclass----nombre_clase_dispositivo-'

>----->
      '-PLANPrefix----prefijo-'  '-INSTRPrefix----prefijo-'

>----->
      |               .-,------. |
      |               V              | |
      '-COPYstgpool-----nombre_agrupación--+'

>----->
      |               .-,------. |
      |               V              | |
      '-ACTIVEDatastgpool-----nombre_agrupación--+'

>----->
      |               .-,------. |
      |               V              | |
      '-PRIMstgpool-----nombre_agrupación--+'

.-Wait----No-----
>-----><
      '-Wait----+No--+-'
              '-Yes-'

```

Parámetros

Source

Especifica el tipo de serie de copias de seguridad de base de datos que IBM Spectrum Protect presupone cuando se genera el archivo del plan de recuperación. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Las opciones son:

DBBackup




Especifica que IBM Spectrum Protect presupone la última serie de copias de seguridad de base de datos completas.

DBSnapshot

Especifica que IBM Spectrum Protect presupone la última serie de copias de seguridad de instantánea de base de datos.

DEVclass

Especifica el nombre de clase de dispositivo que se utiliza para crear un objeto de archivo del plan de recuperación en un servidor destino. La clase de dispositivo debe tener un tipo de dispositivo SERVER.
Importante: La capacidad máxima de la clase de dispositivo debe ser mayor que el tamaño del archivo del plan de recuperación. Si el tamaño del archivo del plan de recuperación sobrepasa la capacidad máxima, el mandato no se ejecuta.
El convenio de denominación del objeto de archivo que contiene el archivo del plan de recuperación en el servidor destino es:

- **Nombre de espacio de archivos:**
 - ADSM.SERVER
- **Calificador de alto nivel:**
 -  Sistemas operativos AIX  Sistemas operativos Linuxprefijoclasedisp/nombreservidor.aaaammdd.hhmmss
 -  Sistemas operativos Windowsprefijoclasedisp\nombreservidor.aaaammdd.hhmmss
- **Calificador de bajo nivel:**
 - RPF.OBJ.1




El nombre de volumen virtual del archivo del plan de recuperación grabado en la tabla de archivos históricos de volúmenes del servidor de origen tiene el formato `nombreservidor.aaaammdd.hhmmss`.


Si no se especifica el parámetro DEVCLASS, el archivo del plan de recuperación se grabará en un archivo según el prefijo del plan.

Si se especifica SOURCE=DBBACKUP, o se ha tomado como valor predeterminado, la entrada de la información histórica de volúmenes para el objeto de archivo del plan de recuperación especifica un tipo de volumen de RPFIL. Si se especifica SOURCE=DBSNAPSHOT, la entrada de la información histórica de volúmenes especifica un tipo de volumen de RPFNSAPSHOT.

PLANPrefix

Especifica el prefijo de nombre de ruta que se utiliza en el nombre de archivo del plan de recuperación. Este parámetro es opcional.

-  Sistemas operativos AIX  Sistemas operativos LinuxLa longitud máxima es de 250 caracteres.
-  Sistemas operativos WindowsLa longitud máxima son 200 caracteres.

 Sistemas operativos WindowsEspecifica el prefijo de nombre de ruta que se utiliza en el nombre de archivo del plan de recuperación.

IBM Spectrum Protect agrega al prefijo la información de fecha y hora ordenable con el formato `aaaammdd.hhmmss`. Por ejemplo: 20081115.051421.

 Sistemas operativos AIX  Sistemas operativos LinuxEl prefijo puede ser uno de los siguientes:

Ruta del directorio

Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
PLANPREFIX=/admsrv/recplans/
```

El nombre de archivo resultante sería:

```
/admsrv/recplans/20081115.051421
```

Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
PLANPREFIX=/admsrv/recplans/accounting
```

El nombre de archivo resultante sería:

```
/admsrv/recplans/accounting.20081115.051421
```

Observe el punto antes de la fecha y la hora.

Sólo serie


IBM Spectrum Protect especifica la ruta del directorio. IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es `/opt/tivoli/tsm/server/bin` y se especifica el parámetro siguiente:

```
PLANPREFIX=shipping
```

El nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.20081115.051421
```

Observe el punto antes de la fecha y la hora.

 Sistemas operativos WindowsEl prefijo puede ser uno de los siguientes:

Ruta del directorio

Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
PLANPREFIX=c:\admsrv\recplans\
```

El nombre de archivo resultante sería:

```
c:\admsrv\recplans\20081115.051421
```

Consejo: Si emite el mandato PREPARE desde el cliente de línea de mandatos de administración y el último carácter de la línea de mandatos es una barra inclinada invertida, se interpretará que ésta es un carácter de continuación. Para evitar esto, especifique el valor del prefijo entre comillas dobles. Por ejemplo:

```
PLANPREFIX="c:\admsrv\recplans\"
```

Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
PLANPREFIX=c:\admsrv\recplans\accounting
```

El nombre de archivo resultante sería:

```
c:\admsrv\recplans\accounting.20081115.051421
```

Observe el punto antes de la fecha y la hora.

Sólo serie


IBM Spectrum Protect agrega la fecha y la hora con el formato *.aaaammdd.hhmmss* (observe el punto antes de la fecha y la hora) al prefijo. La ruta del directorio que utiliza el mandato PREPARE es el directorio que representa esta "instancia" del servidor de IBM Spectrum Protect. Normalmente, este directorio es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, el directorio que representa a esta instancia del servidor es `c:\Archivos de programa\Tivoli\TSM;\server2`, y se emite el mandato PREPARE con el parámetro siguiente:

```
PLANPREFIX=shipping
```

El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.20081115.051421
```



Si no se especifica el parámetro PLANPREFIX, IBM Spectrum Protect selecciona el prefijo de uno de estos modos:

- Si se ha emitido el mandato SET DRMPREFIX, IBM Spectrum Protect utiliza el prefijo que se ha especificado en ese mandato.
-  Sistemas operativos Windows Si no se ha definido el mandato SET DRMPREFIX, IBM Spectrum Protect utiliza como ruta el directorio que representa a esta "instancia" del servidor de IBM Spectrum Protect que, por lo general, es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, si el directorio que representa esta instancia del servidor es el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2\20081115.051421
```


-  Sistemas operativos AIX  Sistemas operativos Linux Si no se ha emitido el mandato SET DRMPREFIX, IBM Spectrum Protect utiliza el nombre de ruta de directorio del directorio de trabajo actual. Por ejemplo, el directorio actual de trabajo es el siguiente:


```
/opt/tivoli/tsm/server/bin
```



El nombre de archivo resultante sería:

```
/opt/tivoli/txm/server/bin/20081115.051421
```

INSTRPrefix

Especifica el prefijo del nombre de ruta que utiliza IBM Spectrum Protect para localizar los archivos que contienen las instrucciones de recuperación. La longitud máxima son  Sistemas operativos AIX  Sistemas operativos Linux 250

 Sistemas operativos Windows 200 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux El prefijo puede ser uno de los siguientes:

Ruta del directorio

Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
INSTRPREFIX=/admsrv/recinstr/
```

```
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
INSTRPREFIX=/admsrv/recinstr/accounts
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```


Sólo serie

- IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es /opt/tivoli/tsm/server/bin y se especifica el parámetro siguiente:

```
INSTRPREFIX=shipping
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```

 Sistemas operativos Windows El prefijo puede ser uno de los siguientes:

Ruta del directorio

Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
INSTRPREFIX=c:\admsrv\recinstr\
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

Consejo: Si emite el mandato PREPARE desde el cliente de línea de mandatos de administración y el último carácter de la línea de mandatos es una barra inclinada invertida, se interpretará que ésta es un carácter de continuación. Para evitar esto, especifique el valor del prefijo entre comillas dobles. Por ejemplo:

```
INSTRPREFIX="c:\admsrv\recinstr\"
```

Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
INSTRPREFIX=c:\admsrv\recinstr\accounts
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

Sólo serie


IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación al prefijo. Si el prefijo sólo es una serie, la ruta del directorio que utiliza el mandato PREPARE es el directorio que representa a esta instancia del servidor de IBM Spectrum Protect. Normalmente, es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, el directorio que representa a esta instancia del servidor es c:\Archivos de programa\Tivoli\TSM;\server2, y se emite el mandato PREPARE con el parámetro siguiente:

```
INSTRPREFIX=dock
```

El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.20081115.051421
```

Si no especifica el parámetro INSTRPREFIX, IBM Spectrum Protect selecciona el prefijo de uno de estos modos:


- Si se ha emitido el mandato SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza el prefijo que se ha especificado en ese mandato.
-  Sistemas operativos Windows Si no se ha emitido el mandato SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza como ruta el directorio que representa a esta "instancia" del servidor de IBM Spectrum Protect que, por lo general, es el

directorio de instalación original del servidor. Por ejemplo, si el directorio que representa esta instancia del servidor es el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2\RECOVERY.INSTRUCTIONS.GENERAL
```

-  Sistemas operativos AIX/Sistemas operativos Linux Si no se ha emitido el mandato SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza el directorio de trabajo actual.

Por ejemplo, si el directorio de trabajo actual es /opt/tivoli/tsm/server/bin, para el archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/RECOVERY.INSTRUCTIONS.GENERAL
```

PRIMstgpool

Especifica los nombres de las agrupaciones de almacenamiento primarias que desea restaurar. Puede separar los nombres de las agrupaciones de almacenamiento con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si se ha emitido el mandato SET DRMPRIMSTGPOOL, IBM Spectrum Protect incluye las agrupaciones de almacenamiento primarias que se indican en ese mandato.
- Si no se ha emitido el mandato SET DRMPRIMSTGPOOL, IBM Spectrum Protect incluye todas las agrupaciones de almacenamiento primarias.

COPYstgpool

Especifica los nombres de las agrupaciones de almacenamiento de copia utilizadas para hacer copia de seguridad de las agrupaciones de almacenamiento primarias que desea restaurar (consulte el parámetro PRIMSTGPOOL). Puede separar los nombres de las agrupaciones de almacenamiento con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si se ha emitido el mandato SET DRMCOPYSTGPOOL, IBM Spectrum Protect incluye esas agrupaciones de almacenamiento de copia.
- Si no se ha emitido el mandato SET DRMCOPYSTGPOOL, IBM Spectrum Protect incluye todas las agrupaciones de almacenamiento de copia.

ACTIVEDatstgpool

Especifica los nombres de las agrupaciones de almacenamiento de datos activos que desea que estén disponibles para el acceso fuera del local. Separe los nombres de agrupaciones de almacenamiento de datos activos con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si el mandato SET ACTIVEDATSTGPOOL se había emitido anteriormente con nombres de agrupaciones de almacenamiento de datos activos válidos, IBM Spectrum Protect procesará esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET ACTIVEDATSTGPOOL o si todas las agrupaciones de almacenamiento de datos activos se han eliminado con el mandato SET ACTIVEDATSTGPOOL, IBM Spectrum Protect procesará únicamente los volúmenes de agrupación de almacenamiento que se habían marcado en el local en el momento de ejecutarse el mandato PREPARE. IBM Spectrum Protect marcará estos volúmenes como UNAVAILABLE.

Wait


Especifica si el mandato se procesa de forma subordinada o en primer plano.

No

Especifica el proceso subordinado. Este es el valor predeterminado.

Yes

Especifica el proceso en primer plano.

 Sistemas operativos AIX/Sistemas operativos Linux No se puede especificar YES desde la consola del servidor.

Ejemplo: crear un archivo de plan de recuperación

Emitir el mandato PREPARE y consultar las anotaciones de actividades para comprobar los resultados.

```
prepare  
query actlog search=prepare
```

 Sistemas operativos AIX/Sistemas operativos Linux

```

05/03/2008 12:01:13 ANR0984I Proceso 3 para PREPARE iniciado en
BACKGROUND a las 12:01:13.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.DATABASE.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.STGPOOL.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEP.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEPSM.
05/03/2008 12:01:14 ANR6920W PREPARE: El nombre de volumen de
sustitución generado, BACK4X@ no es
válido para el tipo de dispositivo
8MM. Nombre de volumen original: BACK4X. Sección:
la macro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14 ANR6900I PREPARE: Se ha creado el archivo de
plan de recuperación
/home/guest/drmtest/prepare/plandir/DSM1509/
r.p.20080503.120113.
05/03/2008 12:01:14 ANR0985I El proceso 3 para PREPARE ejecutado en
BACKGROUND se ha completado con el estado de
terminación
SUCCESS a las 12:01:14.

```

Sistemas operativos Windows

```

05/03/2008 12:01:13 ANR0984I Proceso 3 para PREPARE iniciado en
BACKGROUND a las 12:01:13.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.DATABASE
no encontrado.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.STGPOOL
no encontrado.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEP.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEPSM.
05/03/2008 12:01:14 ANR6920W PREPARE: El nombre de volumen de
sustitución generado, BACK4X@ no es
válido para el tipo de dispositivo ADSM
Nombre de volumen original: BACK4X. Sección:
la macro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14 ANR6900I PREPARE: Se ha creado el archivo de
plan de recuperación
c:\drmtest\prepare\r.p.20080503.120113
05/03/2008 12:01:14 ANR0985I El proceso 3 para PREPARE ejecutado en
BACKGROUND se ha completado con el estado de
terminación
SUCCESS a las 12:01:14.




```

Mandatos relacionados

Tabla 1. Mandatos relacionados con PREPARE

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.
QUERY RPFFILE	Muestra información sobre archivos del plan de recuperación.

Mandato	Descripción
QUERY SERVER	Muestra información sobre servidores.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMINSTRPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta de las instrucciones del plan de recuperación.
SET DRMPPLANVPOSTFIX	Especifica los nombres de los volúmenes de sustitución del archivo del plan de recuperación.
SET DRMPPLANPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta del plan de recuperación.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

Utilice este mandato para proteger los datos de una agrupación de almacenamiento de contenedores de directorio almacenando una copia de los datos en otra agrupación de almacenamiento en un servidor de destino de duplicación o en el mismo servidor protegiendo los datos en cinta. Cuando protege la agrupación de almacenamiento de contenedores de directorio, puede intentar posteriormente reparar los daños en la agrupación de almacenamiento mediante el mandato REPAIR STGPOOL.

Cuando emite el mandato PROTECT STGPOOL para una agrupación de almacenamiento de contenedores de directorio, se realiza una copia de seguridad de los datos almacenados en esa agrupación de almacenamiento en el destino que especifique. La copia de seguridad de los datos se puede realizar en los tipos de destino siguientes:

- Una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino.
Requisito previo: Para la agrupación de almacenamiento que se protege, debe especificar la agrupación de destino mediante el parámetro PROTECTSTGPOOL del mandato DEFINE STGPOOL o UPDATE STGPOOL.

Cuando se utiliza regularmente el mandato PROTECT STGPOOL, normalmente puede reducir el tiempo de proceso para el mandato REPLICATE NODE. Las extensiones de datos que ya se han copiado en el servidor de réplica de destino a través de las operaciones de protección de agrupación de almacenamiento se omiten cuando se inicia la réplica.

Como parte de la operación PROTECT STGPOOL, pueden ejecutarse procesos para reparar extensiones dañadas en la agrupación de almacenamiento del servidor de destino. La operación de reparación se realiza bajo las condiciones siguientes:

- Tanto el servidor de origen como el servidor de destino deben estar en la versión V7.1.5 o posterior.
- Las extensiones que ya se han marcado como dañadas en el servidor de destino se reparan. El proceso de reparación no ejecuta un proceso de auditoría para identificar el daño.
- Sólo se reparan las extensiones de destino que coinciden con las extensiones de origen. Las extensiones de destino dañadas pero que no tienen coincidencia en el servidor de origen no se reparan.

Limitaciones: La operación de reparación que se ejecuta como parte de la operación PROTECT STGPOOL tiene las limitaciones siguientes:

- Las extensiones que pertenecen a los objetos cifrados no se reparan.
- El momento de la aparición de daños en la agrupación de almacenamiento de destino y la secuencia de los mandatos REPLICATE NODE y PROTECT STGPOOL puede afectar al éxito del proceso de reparación. Es posible que algunas extensiones almacenadas en la agrupación de almacenamiento de destino por un mandato REPLICATE NODE no se reparen.

- Agrupaciones de almacenamiento de copia de contenedor en el mismo servidor, protegidas en cinta.
Requisito previo: Para la agrupación de almacenamiento que se está protegiendo, debe especificar la agrupación de almacenamiento de destino utilizando el parámetro PROTECTLOCALSTGPools. Para conocer los detalles sobre el parámetro,

consulte los mandatos para definir y actualizar las agrupaciones de almacenamiento de contenedores de directorio (mandatos DEFINE STGPOOL y UPDATE STGPOOL).

Como parte de la operación PROTECT STGPOOL, se pueden reclamar los volúmenes de la agrupación de directorios. El valor del parámetro RECLAIM de la agrupación de almacenamiento de copia de contenedor afecta a si se reclaman los volúmenes. Para obtener detalles sobre el parámetro, consulte los mandatos para definir y actualizar agrupaciones de almacenamiento de copia de contenedor (mandatos DEFINE STGPOOL y UPDATE STGPOOL).

Restricción: No puede programar distintas operaciones de PROTECT STGPOOL para ejecutarlas simultáneamente. Espere a que una operación PROTECT STGPOOL finalice antes de iniciar otra.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis cuando el destino es el servidor de réplica

```
>>-PROTECT STGPool--agrup_almac_origen----->
. -Type-----Replserver-.  .-FORCEREConcile-----No-----
>+-----+-----+-----+-----+----->
'-Type-----Replserver-'  '-FORCEREConcile-----+No--+-'
                                     '-Yes-'



                                (1)

. -MAXSESSions-----10-----
>+-----+-----+-----+-----+----->
'-MAXSESSions-----+-----+-----+-----+-----'
                                     '-Yes-'

. -Preview ----No----- . -PURGEdata----No-----
>+-----+-----+-----+-----+----->
'-Preview-----+No--+-'  '-PURGEdata-----+No-----+'
                                     '+-All-----+'
                                     '-Deleted-'

. -Wait-----No----- . -TRANSFERMethod-----Tcpi-----
>+-----+-----+-----+-----+-----><
'-Wait-----+No--+-'  |                                     (2) |
                                     '-TRANSFERMethod-----+Tcpi+-----+'
                                     '-Fasp--'
                                     '-Fasp--'
```

Notas:

1.  Sistemas operativos Linux Si el parámetro TRANSFERMETHOD se establece en el valor predeterminado de TCPIP, el valor predeterminado del parámetro MAXSESSIONS es 10. Si el parámetro TRANSFERMETHOD se establece en FASP, el valor predeterminado del parámetro MAXSESSIONS es 2.
2.  Sistemas operativos Linux El parámetro TRANSFERMETHOD solo está disponible en sistemas operativos Linux x86_64 .

Sintaxis cuando el destino es una agrupación de almacenamiento de cinta en el mismo servidor

```
>>-PROTECT STGPool--agrup_almac_origen--Type-----Local----->
. -Preview ----No----- . -RECLaim-----Yes-----
>+-----+-----+-----+-----+----->
'-Preview-----+No--+-'  '-RECLaim-----+Yes-----+'
                                     '+-No-----+'
                                     '+-Only-----+'
                                     '+-YESLIMited--+'
                                     '-ONLYLIMited-'

. -Wait-----No-----
>+-----+-----+-----+-----+-----><
'-Wait-----+No--+-'
                                     '-Yes-'
```

Parámetros

agrup_almac_origen (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen.

Type

Especifica el tipo de destino para la operación de protección. Este parámetro es opcional. El valor predeterminado es REPLSERVER. Especifique uno de los siguientes valores:

Replserver

Especifica que el destino es la agrupación de almacenamiento en el servidor de destino de réplica, tal como se define para la agrupación de almacenamiento de origen con el parámetro PROTECTSTGPOOL en el mandato DEFINE STGPOOL o UPDATE STGPOOL.

Local

Especifica que el destino está en el mismo servidor que la agrupación de almacenamiento de origen. El destino es la agrupación de almacenamiento de copia de contenedor definida para la agrupación de almacenamiento de origen con el parámetro PROTECTLOCALSTGPools en el mandato DEFINE STGPOOL o UPDATE STGPOOL.
Consejo: De forma predeterminada, el servidor utiliza un máximo de dos procesos paralelos para copiar datos a un destino local. Puede cambiar el número máximo de procesos paralelos actualizando la agrupación de almacenamiento de copia de contenedor que es el destino. Utilice el mandato UPDATE STGPOOL con el parámetro PROTECTPROCESS.

FORCEREconcile

Especifica si se deben conciliar las diferencias entre las extensiones de datos de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen y el servidor de destino. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No



Especifica que la copia de seguridad de los datos no compara todas las extensiones de datos de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen con las extensiones de datos en el servidor de destino. En su lugar, la copia de seguridad de los datos realiza un seguimiento de los cambios en las extensiones de datos del servidor de origen desde la última copia de seguridad, y los sincroniza en el servidor de destino.

Yes

Especifica que la copia de seguridad de los datos compara todas las extensiones de datos en el servidor de origen con las extensiones de datos en el servidor destino, y sincroniza las extensiones de datos en el servidor de destino con el servidor de origen.

MAXSESSions

Especifica el número máximo de sesiones de datos que pueden enviar datos a un servidor de destino. Este parámetro es opcional. El valor que se especifique puede estar en el rango de 1 a 100.

 Sistemas operativos AIX  Sistemas operativos Windows El valor predeterminado es 10.

 Sistemas operativos Linux El valor predeterminado varía:

- Si TRANSFERMETHOD=TCPIP, el valor predeterminado del parámetro MAXSESSIONS es 10.
- Si TRANSFERMETHOD=FASP, el valor predeterminado del parámetro MAXSESSIONS es 2.

Si aumenta el número de sesiones, puede mejorar el rendimiento para la agrupación de almacenamiento.

Cuando establezca un valor para el parámetro MAXSESSIONS, asegúrese de que el ancho de banda disponible y la capacidad del procesador de los servidores de origen y de destino sean suficientes.

Consejos:

- Si emite un mandato QUERY SESSION, el número total de sesiones puede superar el número de sesiones de datos. La diferencia se debe a las sesiones de control breves que se utilizan para consultar y configurar operaciones.
- El número de sesiones que se utilizan para la protección depende de la cantidad de datos que se han copiado. Si hace copia de seguridad solamente de una cantidad pequeña de datos, el aumento del número de sesiones no proporciona beneficio.

Preview

Especifica si se obtiene una vista previa de los datos. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No

Especifica que se realiza una copia de seguridad de los datos en el servidor de destino, pero no se obtiene una vista previa de los datos.

Yes

Especifica que se obtiene una vista previa de los datos, pero no se realiza una copia de seguridad.

PURGEdata

Especifica que las extensiones de datos se suprimen del servidor de destino. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que las extensiones de datos no se suprimen del servidor de destino.

All

Especifica que todas las extensiones de datos se suprimen del servidor de destino. Las extensiones de datos a las que se hace referencia en otros datos en la agrupación de almacenamiento de destino no se suprimen.

Deleted

Especifica que las extensiones de datos que se han suprimido en el servidor de origen se suprimen del servidor de destino. Las nuevas extensiones de datos no están protegidas.

RECLaim

Especifica si se ejecuta una reclamación cuando se procesa el mandato PROTECT STGPOOL. La reclamación se ejecuta en la agrupación de almacenamiento de copia de contenedor local que es el destino de la operación de protección. Este parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que la reclamación se ejecuta cuando se emite el mandato, junto con la operación de protección de la agrupación de almacenamiento. La reclamación se ejecuta hasta finalizar, sin limitaciones relativas a la cantidad de volúmenes de la agrupación de almacenamiento que se procesan para la reclamación.

No

Especifica que la reclamación no se ejecuta cuando se emite el mandato. Solo se ejecuta la protección de la agrupación de almacenamiento.

Only

Especifica que la reclamación es la única operación que se ejecuta cuando se emite el mandato. La operación de protección de la agrupación de almacenamiento no se ejecuta, de modo que los datos de la agrupación de almacenamiento de contenedores de directorio que se hayan actualizado desde la última operación de protección no se protegerán. La reclamación se ejecuta hasta finalizar, sin limitaciones relativas a la cantidad de volúmenes de la agrupación de almacenamiento que se procesan para la reclamación.

YESLIMited

Especifica que la reclamación se ejecuta cuando se emite el mandato, junto con la operación de protección de la agrupación de almacenamiento. La reclamación se ejecuta hasta que se alcanza el límite de reclamación que se ha definido para la agrupación de almacenamiento de copia de contenedor. El límite de reclamación se define con el parámetro RECLAIMLIMIT en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

ONLYLIMited

Especifica que la reclamación es la única operación que se ejecuta cuando se emite el mandato. La operación de protección de la agrupación de almacenamiento no se ejecuta, de modo que los datos de la agrupación de almacenamiento de contenedores de directorio que se hayan actualizado desde la última operación de protección no se protegerán. La reclamación se ejecuta hasta que se alcanza el límite de reclamación que se ha definido para la agrupación de almacenamiento de copia de contenedor. El límite de reclamación se define con el parámetro RECLAIMLIMIT en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

Wait

Especifica si se debe esperar a que el servidor procese este mandato en primer plano. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:


No


Especifica que el mandato se procesa en segundo plano. Para supervisar los procesos en segundo plano de este mandato, emita el mandato QUERY PROCESS.

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

Restricción: No se puede especificar `WAIT=YES` desde la consola del servidor.

 Sistemas operativos LinuxTRANSFERMethod

 Sistemas operativos LinuxEspecifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN). Si especifica `TRANSFERMETHOD=FASP`, altera temporalmente cualquier parámetro `TRANSFERMETHOD` que haya especificado en los mandatos `DEFINE SERVER` o `UPDATE SERVER`.

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si las licencias no se encuentran o han caducado, las operaciones para proteger las agrupaciones de almacenamiento fallan.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.

Ejemplo: suprimir todas las extensiones de datos del servidor de destino

Suprimir todas las extensiones de datos en una agrupación de almacenamiento de contenedores de directorio en el servidor de destino. La agrupación de almacenamiento de contenedores de directorio denominada POOL1 en el servidor de origen ya no está protegida por la agrupación de almacenamiento de contenedores de directorio en el servidor de destino. Puede suprimir todas las extensiones para limpiar la agrupación de almacenamiento de contenedores de directorio en el servidor de destino que ya no protege el servidor de origen.

```
protect stgpool pool1 purgedata=all
```

Ejemplo: proteger una agrupación de almacenamiento y especificar un número máximo de sesiones de datos

Proteja una agrupación de almacenamiento denominada SPOOL1 en el servidor de origen realizando una copia de seguridad de los datos en un servidor de réplica de destino, TPOOL1. Especifique un máximo de 20 sesiones de datos.

```
update stgpool spool1 protectstgpool=tpool1  
protect stgpool spool1 maxsessions=20
```

Ejemplo: copiar los datos de la agrupación de almacenamiento en cinta

Proteja una agrupación de almacenamiento de contenedores de directorio copiando los datos a una agrupación de almacenamiento de copia de contenedor en el mismo servidor. En este ejemplo, la agrupación de almacenamiento de contenedores de directorio se llama SPOOL1 y la agrupación de almacenamiento de copia de contenedor que utiliza cinta para almacenamiento se llama TAPES1.

1. Actualice la agrupación de almacenamiento de contenedores de directorio para añadir TAPES1 como la agrupación de almacenamiento local para protección. La agrupación de almacenamiento TAPES1 debe ser una agrupación de almacenamiento de copia de contenedor. Emita el mandato siguiente:

```
update stgpool spool1 protectlocalstgpools=tapes1
```

2. Proteja los datos de la agrupación de almacenamiento de contenedores de directorio con una copia local emitiendo el mandato siguiente:

```
protect stgpool type=local spool1
```

Los datos se copia en la agrupación de almacenamiento TAPES1.

Ejemplo: reclamar espacio en volúmenes de cinta antes de proteger una agrupación de almacenamiento

Reclame espacio en los volúmenes de cinta utilizados para proteger una agrupación de almacenamiento de contenedores de directorio. A continuación, proteja los datos de la agrupación de almacenamiento de contenedores de directorio. En este ejemplo, la agrupación de almacenamiento de contenedores de directorio se denomina SPOOL1.

1. Reclamar espacio en la agrupación de almacenamiento de copia de contenedor local definida como agrupación de protección de destino para SPOOL1.

```
protect stgpool spool1 type=local reclaim=only
```

2. Proteger los datos en la agrupación de almacenamiento de contenedores de directorio denominada SPOOL1 sin ejecutar la reclamación.

```
protect stgpool spool1 type=local reclaim=no
```

Tabla 1. Mandatos relacionados con PROTECT STGPOOL

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.

Mandato	Descripción
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE STGPOOL (copia de contenedor)	Actualizar una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.

Mandatos QUERY

Utilice los mandatos QUERY para solicitar o visualizar información sobre los objetos de IBM Spectrum Protect.

- QUERY ACTLOG (Consultar las anotaciones de actividades)
- QUERY ADMIN (Visualizar información de administrador)
- QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)
- QUERY ALERTSTATUS (Consultar el estado de una alerta)
- QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)
- QUERY AUDITOCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)
- QUERY BACKUPSET (Consultar un juego de copias de seguridad)
- QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)
- QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)
- QUERY COLLOGROUP (Consultar un grupo de proximidad)
- QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CONTAINER (Consulta de un contenedor)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)
- QUERY COPYGROUP (Consultar grupos de copia)
- QUERY DATAMOVER (visualizar definiciones de un transportador de datos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)
- QUERY DB (Visualizar información de base de datos)
- QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)
- QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)
- QUERY DIRSPACE (Consultar utilización de almacenamiento de directorios FILE)
- QUERY DOMAIN (Consultar un dominio de políticas)
- QUERY DRIVE (Consultar información acerca de una unidad)
- QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)
- QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)
- QUERY ENABLED (Consultar eventos activados)
- QUERY EVENT (Consultar eventos planificados y realizados)
- QUERY EVENTRULES (Consultar reglas para eventos de servidor o de cliente)
- QUERY EVENTSERVER (Consultar el servidor de eventos)
- QUERY EXPORT (Consultar las operaciones de exportación activas o suspendidas)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

- QUERY FILESPACE (Consultar uno o más espacios de archivos)
- QUERY LIBRARY (Consultar una biblioteca)
- QUERY LIBVOLUME (Consultar un volumen de biblioteca)
- QUERY LICENSE (Visualizar información sobre licencias)
- QUERY LOG (Visualizar información sobre el registro de recuperación)
- QUERY MACHINE (Consultar información de máquina)
- QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)
- QUERY MGMTCLASS (Consultar una clase de gestión)
- QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)
- QUERY MONITORSTATUS (Consultar el estado de supervisión)
- QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)
- QUERY NODE (Consultar nodos)
- QUERY NODEDATA (Consultar datos de cliente en volúmenes)
- QUERY NODEGROUP (Consultar un grupo de nodos)
- QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)
- QUERY OPTION (Consultar opciones del servidor)
- QUERY PATH (visualizar una definición de ruta)
- QUERY POLICYSET (Consultar un juego de políticas)
- QUERY PROCESS (Consultar uno o más procesos de servidor)
- QUERY PROFILE (Consultar un perfil)
- QUERY PROTECTSTATUS (Consultar estado de protección de una agrupación de almacenamiento)
- QUERY PROXYNODE (Consulta la autorización de proxy de un nodo cliente)
- QUERY PVUESTIMATE (Mostrar la estimación de unidades de valor de procesador)
- QUERY RECOVERYMEDIA (Consultar medio de recuperación)
- QUERY REPLICATION (Consultar los procesos de réplica de nodos)
- QUERY REPLNODE (Mostrar información sobre el estado de réplica de un nodo de cliente)
- QUERY REPLRULE (Consultar reglas de réplica)
- QUERY REPLSERVER (Consultar un servidor de réplica)
- QUERY REQUEST (Consultar una o más peticiones de montaje pendientes)
- QUERY RESTORE (Consultar sesiones de restauración reiniciables)
- QUERY RPFCONTENT (Consultar el contenido del archivo del plan de recuperación almacenado en un servidor de destino)
- QUERY RPFFILE (Consultar la información del archivo del plan de recuperación almacenado en un servidor de destino)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY SAN (Consultar los dispositivos de la SAN)
- QUERY SCHEDULE (Consultar planificaciones)
- QUERY SCRIPT (Consultar scripts IBM Spectrum Protect)
- QUERY SERVER (Consultar un servidor)
- QUERY SERVERGROUP (Consultar un grupo de servidores)
- QUERY SESSION (Consultar sesiones de cliente)
- QUERY SHREDSTATUS (Consultar estado de destrucción)
- QUERY SPACETRIGGER (Consultar los desencadenantes de espacio)
- QUERY STATUS (Consultar parámetros del sistema)
- QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)
- QUERY STGRULE (Visualizar información de reglas de almacenamiento)
- QUERY STGPOOL (Consultar agrupaciones de almacenamiento)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY STGPOOLDIRECTORY (Consulta de un directorio de agrupaciones de almacenamiento)
- QUERY SUBSCRIBER (Visualizar información de suscriptor)
- QUERY SUBSCRIPTION (Visualizar información de inscripción)
- QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY TAPEALERTMSG (Visualizar estado del mandato SET TAPEALERTMSG)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY TOC (Visualizar tabla de contenido para una imagen de copia de seguridad)
- QUERY VIRTUALFSMAPPING (Consultar una correlación de espacios de archivos virtuales)
- QUERY VOLHISTORY (Visualizar información histórica de volúmenes secuenciales)
- QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)

QUERY ACTLOG (Consultar las anotaciones de actividades)

Utilice este mandato para mostrar los mensajes generados por el servidor y el cliente. Este mandato ofrece diversas opciones de filtro que se pueden utilizar para limitar la cantidad de mensajes visualizados y el tiempo que tarda en procesarse esta consulta. Si no especifica ningún parámetro con este mandato, se visualizarán todos los mensajes generados durante la última hora.

Las anotaciones de actividades contienen todos los mensajes que se han enviado a la consola del servidor en funcionamiento normal. El resultado de los mandatos entrados en la consola del servidor no se graban en las anotaciones de actividades, excepto si el mandato afecta a un proceso subordinado o a una sesión de cliente. Los mensajes de error se visualizan en las anotaciones de actividades.

Restricción: El mandato QUERY ACTLOG no se puede planificar utilizando el mandato DEFINE SCHEDULE.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-BEGINDate---fecha_actual-.
>>-Query ACTlog--+-+-----+----->
      '-BEGINDate---fecha-----'

      .-BEGINTime---hora_actual_menos_1_hora-.
>+-+-----+----->
      '-BEGINTime---hora-----'

      .-ENDDate---fecha_actual-. .-ENDTime---hora_actual-.
>+-+-----+-----+----->
      '-ENDDate---fecha-----' '-ENDTime---hora-----'

>+-+-----+-----+----->
      '-MSGno---numero_mensaje-' '-Search---serie-'

>+-+-----+----->
      '-NODEname---nombre_nodo-'

      .-Originator---ALL-----,
>+-+-----+-----><
      '-Originator---+ALL-----'
          +-Server-----+
          '-Client--| A |-'

A

|+-+-----+----->
      '-OWNERname---nombre_propietario-'

>+-+-----+----->
      '-SCHedname---nombre_planificación-'

>+-+-----+----->
      '-Dmainname---nombre_dominio-'

>+-+-----+-----|
      '-SESSnum---numero_sesión-'

```

Parámetros

BEGINDate

Especifica la fecha inicial del rango de los mensajes que se han de visualizar. Se visualizan todos los mensajes que se ajusten a los criterios de rango horario que se han producido con posterioridad a esta fecha. El valor predeterminado es la fecha actual. Este parámetro es opcional.

Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para visualizar la información empezando por los mensajes creados hace una semana, puede especificar BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango de los mensajes que se han de visualizar. Se visualizan todos los mensajes que se ajusten a los criterios de rango horario que se han producido con posterioridad a esta hora. Si no especifica la hora, se visualizarán todos los mensajes que se han producido durante la última hora.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, IBM Spectrum Protect visualizará los mensajes con la hora 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00. Si emite el mandato QUERY ACTLOG a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect visualiza los mensajes con la hora 5:30 o posterior en la fecha inicial.

ENDDate

Especifica la fecha final del rango de los mensajes que se han de visualizar. Se visualizarán todos los mensajes, que reúnan el criterio de rango horario, que se hayan producido antes de esta fecha. Si no especifica un valor, se utilizará la fecha actual. Este parámetro es opcional.

Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para visualizar la información creada hasta ayer, puede especificar ENDDATE=TODAY-1, o simplemente, ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final del rango de los mensajes que se han de visualizar. Se visualizan todos los mensajes que se ajusten a los criterios de rango horario que se han producido con anterioridad a esta hora. Si no especifica un valor, se visualizarán todos los mensajes hasta la hora en que se ha emitido este mandato. Este parámetro es opcional.

Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, IBM Spectrum Protect visualiza los mensajes con la hora 12:00 o anterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, IBM Spectrum Protect visualizará los mensajes con la hora 5:30 o anterior en la fecha final especificada.

MSGno

Especifica un entero que define el número de mensaje de las anotaciones de actividades que se ha de visualizar. Este entero es sólo la parte numérica del mensaje. Este parámetro es opcional.

Search

Especifica una serie de texto que desea buscar en las anotaciones de actividades. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

Nota: No escriba como una serie de texto el nombre del servidor de IBM Spectrum Protect ni texto con un carácter comodín para buscar el nombre del servidor. De hacerlo, la salida incluirá mensajes que no contendrán la serie de búsqueda.

NODename

Especifica que la consulta visualiza los mensajes que se han anotado para este nodo. Si no especifica un valor para este parámetro, se muestran los mensajes de todos los nodos.

ORiginator

Especifica que la consulta visualiza los mensajes que ha anotado el servidor, el cliente o ambos. El valor predeterminado es ALL. Los valores posibles son:

ALL

Especifica que la consulta visualiza los mensajes que se han originado en el cliente y en el servidor.

SErver

Especifica que la consulta visualiza los mensajes que se han originado en el servidor.

CLient

Especifica que la consulta visualiza los mensajes que se han originado en el cliente.

Puede especificar uno de los valores siguientes para minimizar el tiempo de proceso al consultar en las anotaciones de actividades los mensajes que ha anotado el cliente:

OWNERname

Especifica que la consulta visualiza los mensajes que se han anotado para un propietario concreto. Si no especifica ningún valor en este parámetro, se visualizan los mensajes de todos los propietarios.

SCHedname

Especifica que la consulta visualiza los mensajes que una actividad de cliente planificada concreta ha anotado. Si no especifica ningún valor para este parámetro, se muestran los mensajes de todas las planificaciones.

DOmainname

Especifica que la consulta visualiza los mensajes que se han anotado para un dominio de políticas concreto al que pertenece la planificación indicada. Este parámetro es opcional, a menos que especifique un nombre de planificación.

SESsnum

Especifica que la consulta visualiza los mensajes que se han anotado a partir de un número de sesión de cliente concreto. Si no especifica ningún valor para este parámetro, se visualizan los mensajes de todas las sesiones de cliente.

Ejemplo: buscar en las anotaciones de actividades mensajes que contengan texto específico

Buscar en el registro de actividades los mensajes que contengan la serie "suprimir". La salida incluirá únicamente los mensajes generados durante la última hora. Emita el mandato:

```
query actlog search=suprimir
```

Fecha/Hora	Mensaje
27/08/1998 15:19:43	ANR0812I La caducidad de archivos de clientes del inventario se ha completado: 0 archivos suprimidos.

Ejemplo: buscar en las anotaciones de actividades los mensajes que se han generado dentro de un período de tiempo específico

Visualizar los mensajes que se produjeron ayer entre las 9:30 y las 12:30. Emita el mandato:

```
query actlog begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Fecha/Hora	Mensaje
21/10/1998 10:52:36	ANR0407I Sesión 3921 iniciada para administrador ADMIN (WebBrowser) (HTTP 9.115.20.100(2315)).
21/10/1998 11:06:08	ANR0405I Sesión 3922 finalizada para administrador ADMIN (WebBrowser).
21/10/1998 12:16:50	ANR0405I Sesión 3934 finalizada para administrador ADMIN (WebBrowser).

Ejemplo: buscar en las anotaciones de actividades los mensajes de un nodo de cliente específico

Buscar en las anotaciones de actividades los mensajes de IBM Spectrum Protect originados en el cliente para el nodo JEE. Emita el mandato:

```
query actlog originator=client node=jee
```

Fecha/Hora	Mensaje
10/06/1998 15:46:22	ANE4007E (Núm. sesión: 3 Nodo: JEE) Error al procesar '/jee/report.out': denegado acceso al objeto
11/06/1998 15:56:56	ANE4009E (Núm. sesión: 4 Nodo: JEE) Error al procesar '/jee/work.lst': condición de disco lleno

Ejemplo: buscar en las anotaciones de actividades los mensajes de cliente y servidor de un nodo de cliente y sesión específicos

Buscar en el registro de actividades los mensajes de IBM Spectrum Protect del cliente y el servidor para el nodo A asociado con la sesión 1. La salida incluye todos los mensajes con la cadena de texto definida, SESSION: 1". Emita el mandato:

```
query actlog search="(SESSION:1)"
```

Fecha/Hora	Mensaje
02/13/2012 12:13:42	ANR0406I Sesión 1 iniciada para el nodo A (WinNT)

```

(Tcp/Ip colind(2463)). (SESSION: 1)
02/13/2012 12:13:56 ANE4952I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos inspeccionados: 34
(SESSION: 1)
02/13/2012 12:13:56 ANE4954I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos de copia de seguridad: 34
(SESSION: 1)
02/13/2012 12:13:56 ANE4958I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos actualizados: 0
(SESSION: 1)
02/13/2012 12:13:56 ANE4964I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Tiempo transcurrido en el proceso: 00:00:02
(SESSION: 1)
02/13/2012 12:13:59 ANR0403I La sesión 1 finalizada para nodo A (WinNT).
(SESSION: 1)

```

Ejemplo: Buscar registro de actividad de los mensajes generados por el cliente de una sesión de cliente

Buscar en el registro de actividades los mensajes de IBM Spectrum Protect de una sesión de cliente específica. La salida incluirá únicamente los mensajes generados por el cliente. Emita el mandato:

```
query actlog sessnum=1
```

```

Fecha/Hora      Mensaje
-----
02/13/2012 12:13:56 ANE4952I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos inspeccionados: 34
(SESSION: 1)
02/13/2012 12:13:56 ANE4954I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos de copia de seguridad: 34
(SESSION: 1)
02/13/2012 12:13:56 ANE4958I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Número total de objetos actualizados: 0
(SESSION: 1)
02/13/2012 12:13:56 ANE4964I (ANE4985I Sesión: 1, ANE4986I Nodo: A)
Tiempo transcurrido en el proceso: 00:00:02
(SESSION: 1)

```

Descripciones de los campos

Date/Time

Especifica la fecha y hora en la que el servidor o el cliente generó el mensaje.

Mensaje

Especifica el mensaje que generó el servidor o el cliente.

Mandatos relacionados

Tabla 1. Mandato relacionado con QUERY ACTLOG

Mandato	Descripción
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.

QUERY ADMIN (Visualizar información de administrador)

Utilice este mandato para visualizar información acerca de uno o más administradores.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

.-*-----
>>-Query Admin----->
'-nombre_admin-'

```


Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

Ejemplo: visualizar información acerca de todos los administradores

Visualizar información parcial acerca de todos los administradores. Emita el mandato:

```
query admin
```

Nombre administrador	Días desde último	Días desde asignación	Bloqueo acceso	Clases privilegio contraseña
ADMIN	<1	<1	No	Sistema
SERVER_CONSOLE			No	Sistema

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información completa acerca de un administrador

Desde un servidor gestionado, visualizar información completa del administrador denominado ADMIN. Emita el mandato:

```
query admin admin format=detailed
```

```
Nombre administrador: ADMIN
Fecha/hora último acceso: 1998.06.04 17.10.52
Días desde último acceso: <1
Fecha/hora asignación contraseña: 1998.06.04 17.10.52
Días desde asignación contraseña: 26
Número conexiones no válidas: 0
Bloqueo: No
Contacto:
Privilegio de sistema: Sí
Privilegio de políticas: **Incluido con privilegio de sistema**
Privilegio de almacenamiento: **Incluido con privilegio de sistema**
Privilegio de operador: **Incluido con privilegio de sistema**
Privilegio de acceso a cliente: **Incluido con privilegio de sistema**
Privilegio de propietario de cliente: **Incluido con privilegio de sistema**
Fecha/hora registro: 05/09/1998 23:54:20
Inscrito por administrador: SERVER_CONSOLE
Perfil de gestión:
Período caducidad contraseña: 90 día(s)
Dirección de correo electrónico:
Alertas de correo electrónico: Sí
Autenticación: Local
SSL necesario: No
Session Security: Strict
Transport Method: TLS 1.2
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre administrador

Especifica el nombre del administrador.

Fecha/hora último acceso

Especifica la fecha y la hora en que el administrador accedió por última vez al servidor.

Días desde último acceso

Especifica el número de días transcurridos desde que el administrador accedió por última vez al servidor.

Fecha/hora asignación contraseña

Especifica la fecha y hora en que se ha definido la contraseña del administrador o de la actualización más reciente.

Días desde asignación contraseña

Especifica el número de días transcurridos desde que se ha definido la contraseña del administrador o desde la actualización más reciente.

Contador de conexiones no válidas

Especifica el número de intentos de inicio de sesión no válidos que se han realizado desde el último inicio de sesión satisfactorio. Este número únicamente no puede ser distinto a cero cuando un límite de contraseña no válida (SET INVALIDPWLIMIT) es mayor que cero. Cuando el número de intentos no válidos es igual al límite establecido mediante el mandato SET INVALIDPWLIMIT, se bloquea el acceso del administrador al sistema.

Bloqueo

Especifica si el administrador tiene bloqueado el acceso al sistema.

Contacto

Especifica cualquier información de contacto para el administrador.

Privilegio sistema

Especifica si se ha otorgado al administrador el privilegio de sistema.

Privilegio política

Especifica si se ha otorgado al administrador privilegio de política sin restricciones o los nombres de cualquier dominio de políticas que pueda gestionar el administrador con privilegio de política con restricciones.

Privilegio almacenamiento

Especifica si se ha otorgado al administrador privilegio sin restricciones de almacenamiento o los nombres de cualquier agrupación de almacenamiento que pueda gestionar el administrador con privilegio de almacenamiento con restricciones.

Privilegio operador

Especifica si se ha otorgado al administrador el privilegio de operador.

Privilegio acceso cliente

Especifica que se ha otorgado autorización de acceso a cliente a un usuario con privilegio de nodo.

Privilegio propietario cliente

Especifica que se ha otorgado autorización de propietario de cliente a un usuario con privilegio de nodo.

Fecha/hora registro

Especifica la fecha y hora en que se ha registrado el administrador.

Registrado por administrador

Especifica el nombre del administrador que ha registrado al administrador. Si este campo contiene \$\$CONFIG_MANAGER\$\$, el administrador está asociado a un perfil que gestiona el gestor de configuración.

Perfil de gestión

Especifica los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este administrador.

Período de caducidad de contraseña

Especifica el período de caducidad de la contraseña del administrador.

Dirección de correo electrónico

Especifica la dirección de correo electrónico del administrador.

Alertas de correo electrónico

Especifica si las alertas se envían al administrador especificado por correo electrónico.

Autenticación

Especifica el método de autenticación de contraseña: LOCAL, LDAP o LDAP (pendiente).

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP
Este administrador está configurado para autenticarse con un servidor de directorio LDAP, pero el administrador aún no se autenticó a través de un nodo de cliente.	LDAP (pendiente)

SSL necesario (en desuso)

Especifica si la configuración de seguridad para el ID de usuario administrador requiere capa de sockets seguros (SSL). Los valores pueden ser SI, NO o predeterminado. Debe tener autorización de nivel de sistema para actualizar el valor de administrador SSLREQUIRED . Este parámetro está en desuso.

Seguridad de sesión

Especifica el nivel de seguridad de sesión que se impone para el ID de administrador. Los valores pueden ser STRICT o TRANSITIONAL.

Método de transporte

Especifica el método de transporte que se ha utilizado la última vez para el administrador especificado. Los valores pueden ser TLS 1.2, TLS 1.1 o NONE. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY ADMIN

Mandato	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.

Mandato	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REMOVE ADMIN	Suprime un administrador de la lista de administradores registrados.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
REVOKE AUTHORITY	Revoca una o más clases de privilegio o limita el acceso a los dominios de políticas y agrupaciones de almacenamiento.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.

QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)

Utilice este mandato para visualizar qué mensajes de servidor se han definido como alertas.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query ALERTTrigger--*-----<
                        +-----+-----<
                        |---número_mensaje---|
```

Parámetros

número_mensaje

Especifica el número de mensaje que desea consultar. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres. Puede utilizar caracteres comodín para especificar números de mensajes. Si no especifica un número de mensaje, se visualizan todos los desencadenantes de alerta.

Consultar desencadenantes de alerta para visualizar qué mensajes se designan como alertas

Visualice todos los mensajes designados como alertas, emitiendo el mandato siguiente:

```
query alerttrigger
```

Ejemplo de salida:

Desencadenante alerta	Categoría	Administrador
ANR1067E	SERVER	HARRYH
ANR1073E	SERVER	CSDADMIN, DJADMIN, HARRYH
ANR1074E	STORAGE	CSDADMIN, DJADMIN, HARRYH
ANR1096E	STORAGE	CSDADMIN, DJADMIN, HARRYH, MHAYE

Consultar desencadenantes de alerta para un número de mensajes específico

LOcal
Visualiza alertas que se han originado en el servidor de IBM Spectrum Protect local.

CLient
Visualiza alertas que se han originado en el cliente de IBM Spectrum Protect.

REmote
Visualiza alertas que se han originado en otro servidor de IBM Spectrum Protect.

SOURCENAME
Especifica el nombre del origen donde se ha originado la alerta. SOURCENAME puede ser el nombre de un servidor de IBM Spectrum Protect local o remoto, o un cliente de IBM Spectrum Protect.

ID
Este parámetro opcional especifica el ID exclusivo de la alerta que desea visualizar. Especifique un valor de 1 a 9223372036854775807.

ASSigned
Especifica el nombre del administrador que se asigna a la alerta que desea consultar.

RESolvedby
Especifica el nombre de administrador que ha resuelto la alerta que desea consultar.

Consultar alertas activas

Muestra solo las alertas que están activas en la base de datos de servidor emitiendo el siguiente mandato:

```
query alertstatus status=active
```

Consultar alertas activas para dos mensajes emitidos por el servidor local

Emita el mandato siguiente para visualizar sólo las alertas activas para los números de mensaje ANE4958I y ANR4952E que han sido emitidos por el servidor local:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=local
```

Consultar alertas activas de los mensajes ANR4958I y ANR4952E emitidos por un cliente

Emita el mandato siguiente para visualizar sólo las alertas activas para los números de mensaje ANE4958I y ANE4952I emitidas por un cliente:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=client
```

Consultar todas las alertas en un servidor

Emita el mandato siguiente para visualizar todas las alertas que hay en el servidor:

```
query alertstatus
```

Salida de ejemplo: Visualizar todas las alertas que hay en el servidor:

```
Identificador de alerta: 83
Número de mensaje de alerta: 293
Nombre origen: SEDONA
Tipo de origen: LOCAL
Primera aparición: 03/07/2013 17:08:35
Última aparición: 03/07/2013 17:08:35
Recuento: 1
Estado: ACTIVE
Último cambio de estado: 12/31/1969 17:00:00
Categoría: INVENTORY
Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla AF_BITFILES.
Asignado:
Resuelto por:
Observación:
```

```
Identificador de alerta: 85
Número de mensaje de alerta: 293
Nombre origen: SEDONA
Tipo de origen: LOCAL
Primera aparición: 03/08/2013 05:45:00
Última aparición: 03/08/2013 05:45:00
Recuento: 1
Estado: ACTIVE
Último cambio de estado: 12/31/1969 17:00:00
```

Categoría: INVENTORY
 Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
 BF_AGGREGATED_BITFILES.
 Asignado:
 Resuelto por:
 Observación:

Identificador de alerta: 1282
 Número de mensaje de alerta: 293
 Nombre origen: ALPINE
 Tipo de origen: LOCAL
 Primera aparición: 02/13/2013 15:47:50
 Última aparición: 02/13/2013 15:47:50
 Recuento: 1
 Estado: CLOSED
 Último cambio de estado: 02/26/2013 09:46:39
 Categoría: INVENTORY
 Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
 TSMMON_ALERT.
 Asignado:
 Resuelto por:
 Observación:

Identificador de alerta: 1792
 Número de mensaje de alerta: 293
 Nombre origen: ALPINE
 Tipo de origen: LOCAL
 Primera aparición: 02/19/2013 08:58:14
 Última aparición: 02/19/2013 08:58:14
 Recuento: 1
 Estado: CLOSED
 Último cambio de estado: 03/01/2013 12:39:21
 Categoría: INVENTORY
 Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
 ACTIVITY_LOG.
 Asignado:
 Resuelto por:
 Observación:

Descripciones de los campos

Identificador de alerta
 Identificador exclusivo de la alerta.

Número de mensaje de alerta
 Número de mensaje de la alerta.

Nombre de origen
 Nombre del origen desde el que se originó la alerta.

Tipo de origen
 Tipo de origen inicial

Primera aparición
 Fecha y hora de la primera aparición de la alerta.

Última aparición
 Fecha y hora de la última aparición de la alerta.

Recuento
 Número total de veces que se ha desencadenado la alerta.

Estado
 Especifica el estado de la alerta.

Último cambio de estado
 Especifica la fecha y la hora a las que cambió por última vez el estado de la alerta.

Categoría
 Categoría de la alerta.

Mensaje
 Mensaje que desencadena la alerta.

Asignado
 Especifica el usuario al que incumbe esta alerta.

Resuelto por
 Especifica el usuario que ha investigado y resuelto la alerta.

Comentarios
 Observación opcional registrada por el solucionador.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY ALERTSTATUS

Mandato	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)

Utilice este mandato para visualizar la información sobre qué nodos cliente están asociados a una o varias planificaciones. Los nodos cliente asociados a una planificación realizan operaciones como, por ejemplo, copia de seguridad o copia archivada, en función de la planificación.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query ASSOCIATION----->
      .-*-----
>+-----+-----><
  |          .-*----- |
  '-nom_dominio-+-----+'
                    '-nombre_planificación-'
```

Parámetros

nombre_dominio

Especifica el nombre del dominio de políticas que se visualizará. Puede utilizar un carácter comodín para especificar este nombre. Se visualizarán todos los nombres de dominios de políticas que coincidan. Si no especifica un valor para este parámetro, se visualizarán todos los dominios de políticas existentes. Si especifica un nombre de dominio, no tiene que especificar un nombre de planificación.

nombre_planificación

Especifica el nombre de la planificación que se visualizará. Puede utilizar un carácter comodín para especificar este nombre. Se visualizarán todos los nombres de planificación que coincidan. Si no especifica un valor para este parámetro, se consultarán todas las planificaciones existentes. Si especifica un nombre de planificación, debe especificar también un nombre de dominio de políticas.

Ejemplo: visualizar los nodos cliente que se asocian a una planificación

Visualizar todos los nodos cliente que están asociados a cada planificación que pertenece al dominio de políticas EMPLOYEE_RECORDS. Emita el mandato:

```
query association employee_records *
Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre planificación: WEEKLY_BACKUP
```

Nodos asociados: JOE JOHNSON LARRY SMITH SMITHERS TOM

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre dominio políticas

Especifica el nombre del dominio de políticas al que pertenece la planificación.

Schedule Name

Especifica el nombre de la planificación.

Nodos asociados

Especifica los nombres de los nodos cliente que están asociados a la planificación indicada.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY ASSOCIATION

Mandato	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DELETE ASSOCIATION	Suprime la asociación entre los clientes y una planificación.

QUERY AUDITOCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)

Utilice este mandato para visualizar información sobre la utilización del almacenamiento del servidor del nodo de cliente. Para visualizar la información de auditoría de licencias actual del servidor, utilice el mandato AUDIT LICENSE antes de emitir el mandato QUERY AUDITOCUPANCY.

Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento de gestión de espacio, de copia de seguridad/archivado que está utilizándose. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de processor y puede atascar otras actividades del servidor. Puede utilizar la opción de servidor AUDITSTORAGE para especificar que no se calcule el almacenamiento como parte de una auditoría de licencia.

Puede utilizar la información de esta consulta para determinar si se debe equilibrar la utilización de almacenamiento de nodos de cliente y dónde debe hacerse. Esta información puede ayudarle en la facturación de clientes por utilización del almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query AUDITOccupancy--+-----+----->
      | .-,------. |
      | v          | |
      |---nombre_nodo+--'

>+-----+----->
      | .-,------. |
      | v          | |
      |---Dmain-----nombre_dominio+--'

.-Pooltype-----ANY-----
>+-----+----->>
      '-Pooltype-----+ANY-----+'
          +-Primary-+
          '-Copy----'
```

Parámetros

nombre_nodo

Especifica una lista de nodos para los que se ha de visualizar la información de utilización del almacenamiento del servidor.

Puede especificar varios nodos separando los nombres de nodos con comas, sin espacios intercalados. Puede utilizar caracteres

comodín para especificar nombres. El valor predeterminado (*) es consultar todos los nodos clientes. Utilice el parámetro DOMAIN para que esta lista se limite a los dominios de políticas. Este parámetro es opcional.

Domain

Especifica una lista de los dominios de políticas para limitar qué nodos se han de visualizar. Se visualizan los nodos que pertenecen a los dominios de políticas especificados. Puede especificar varios dominios de políticas separando los nombres de dominios de políticas con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional.

POoltype

Especifica el tipo de almacenamiento de agrupación de almacenamiento que se visualizará. Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

ANY

Especifica las agrupaciones de almacenamiento primarias y de copia. El valor que se presenta es el total para las dos agrupaciones.

PRimary

Especifica sólo agrupaciones de almacenamiento primarias.

COpy

Especifica sólo agrupaciones de almacenamiento de copia.

Ejemplo: visualizar la utilización del almacenamiento

Visualizar la utilización de almacenamiento combinada de las agrupaciones de almacenamiento primarias y de copia. Emita el mandato:

```
query auditoccupancy
```

Información según última auditoría con fecha 22/05/1996 14:49:51.

Nombre nodo	Copia de seguridad		Archivado gestión espacio (MB)	Espacio gestionado total (MB)	Total
	copias seg. (MB)	copias archivadas			
CLIENT	245	20	0	265	
SMITH	245	20	0	265	
SMITHERS	245	20	0	265	
JOHNSON	300	15	0	320	
JOE	245	20	0	265	
TOM	300	15	0	320	
LARRY	245	20	0	265	

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre del nodo

Especifica el nombre del nodo cliente.

Almacenamiento copias seguridad (MB)

Especifica el uso total de almacenamiento de copia de seguridad para el nodo. Para que este valor, un MB = 1048576 bytes.

Almacenamiento copias archivadas (MB)

Especifica el uso total de almacenamiento de archivos para el nodo. Para que este valor, un MB = 1048576 bytes.

Almacenamiento gestión espacio (MB)

Especifica la cantidad de almacenamiento de servidor que se utiliza para almacenar los archivos que se migran del nodo de cliente mediante un cliente de IBM Spectrum Protect for Space Management. Para que este valor, un MB = 1048576 bytes.

Almacenamiento total utilizado (MB)

Especifica el uso total de almacenamiento para el nodo. Para que este valor, un MB = 1048576 bytes.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY AUDITOCUPANCY

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

Mandato	Descripción
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.

QUERY BACKUPSET (Consultar un juego de copias de seguridad)

Utilice este mandato para visualizar información sobre uno o varios juegos de copias de seguridad.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query BACKUPSET .-*-----+-----+----->
| .-,-----+-----+-----|
| V          | |          | |
|'---+nombre_nodo-----+---+'
|'---nombre_grupo_nodos-'

.*-----+-----+----->
| .-,-----+-----+-----|
| V          | |          | |
|'---nombre_juego_copias_seguridad+---+'

>+-----+-----+-----+-----+----->
|'---BEGINDate---fecha-' |'---BEGINTime---hora-'

>+-----+-----+-----+-----+----->
|'---ENDDate---fecha-' |'---ENDTime---hora-'

>+-----+-----+-----+-----+----->
|'---WHERERetention---dias---+'
|'---NOLimit-'

>+-----+-----+-----+-----+----->
|'---WHEREDESCRIPTION---descripción-'

>+-----+-----+-----+-----+----->
|'---WHEREDEVclass---nombre_clase_dispositivo-'

>+-----+-----+-----+-----+----->
|'---WHERECExists---Yes+---+'
|'---No--'

>+-----+-----+-----+-----+----->
|          .-,-----+-----+-----|
|          V          | |          | |
|'---WHEREDATAType---+FILE---+---+'
|'---IMAGE-'

.-Format---Standard-----+----->
|'---Format---Standard+---+'
|'---Detailed-'

```

Parámetros

nombre_nodo o nombre_grupo_nodos

Especifica el nombre del nodo cliente y grupos de nodos cuyos datos contenidos en el juego de copias de seguridad se van a visualizar. Para especificar varios nombres de nodo y nombres de grupos de nodos, sepárelos con comas y sin espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos.

nombre_juego_copias_seguridad

Especifica el nombre del juego de copias de seguridad cuya información se va a visualizar. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

BEGINDate

Especifica la fecha inicial del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la hora y la fecha. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

ENDDate

Especifica la fecha de finalización del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha finales. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDDATE para especificar una fecha y hora. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique. Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

WHERERetention

Especifica el valor de retención, expresado en días, que debe asociarse a los juegos de copias de seguridad que han de visualizarse. Puede especificar un entero entre el 0 y el 30000. Los valores son:

días

Especifica que los juegos de copias de seguridad que permanecen retenidos durante este número de días, se visualizarán.

NOLimit

Especifica que los juegos de copias de seguridad que permanecen retenidos indefinidamente, se visualizarán.

WHEREDescription

Especifica la descripción que debe estar asociada al juego de copias de seguridad que se va a visualizar. La descripción que especifique puede contener caracteres comodín. Este parámetro es opcional. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

WHEREDEVclass

Especifica el nombre de la clase de dispositivo asociada al juego de copias de seguridad se va a visualizar. Puede utilizar caracteres comodín para especificar un nombre de clase de dispositivo. Este parámetro es opcional.

WHERETOExists

Especifica si un juego de copias de seguridad debe incluir una tabla de contenido para poder visualizarse. Este parámetro es opcional. El valor predeterminado es mostrar todos los juegos de copias de seguridad independientemente de si tienen o no una tabla de contenido.

WHEREDATAType

Especifica el tipo de datos del juego de copias de seguridad que se visualizará. Este parámetro es opcional. El valor predeterminado es visualizar todos los tipos de juegos de copias de seguridad. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados.

FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a visualizar. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad/archivado.

IMAGE

Especifica que se va a visualizar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad/archivado.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Mandato	Descripción
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)

Utilice este mandato para visualizar información acerca de los archivos y directorios que contiene un juego de copias de seguridad para un nodo cliente.

Recuerde: Al procesar este mandato es posible que se utilice una cantidad considerable de recursos de red y de puntos de montaje.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

Sintaxis

```
>>-Query BACKUPSETCONTENTS----->
>--nombre_nodo--nombre_juego_copias_seguridad----->
  .-DATAType---FILE-----
>--+-----+-----><
  '-DATAType---+FILE---+'
      '-IMAGE-'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente cuyos datos contenidos en el juego de copias de seguridad se van a visualizar. El nombre especificado no puede contener caracteres comodín ni puede ser una lista de nombres de nodos separados por comas.

nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a visualizar. El nombre que se especifique no puede contener caracteres comodín ni puede ser una lista de nombres de nodos separados por comas.

DATAType

Especifica que se va a consultar el juego de copias de seguridad que contiene los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que se va a consultar un juego de copias de seguridad de nivel de archivo. Los valores posibles son:

FILE

Especifica que se va a consultar un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad/archivado.

IMAGE

Especifica que se va a consultar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad/archivado.

Ejemplo: consultar el contenido de un juego de copias de seguridad para un nodo específico

Visualizar el contenido del juego de copias de seguridad denominado PERS_DATA.3099 que pertenece al nodo cliente JANE. Emita el mandato:

```
query backupsetcontents jane pers_data.3099
```

Nombre nodo	Espacio archivos	Nombre de archivo del cliente
JANE	/srvr	/deblock
JANE	/srvr	/deblock.c

```
JANE          /srvr      /dsmerror.log
JANE          /srvr      /dsmxxxxx.log
JANE          ...          .....
```

Descripciones de los campos

Node Name

Especifica el nombre del nodo cliente cuyos datos están contenidos en el juego de copias de seguridad.

Filespace Name

Especifica el nombre del espacio de archivos al que pertenece el archivo especificado.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre del archivo en el cliente

Especifica el nombre del archivo.

Los nombres de espacios de archivos y nombres de archivo que pueden estar en una página de códigos o un entorno local diferente de los del servidor no se visualizan correctamente en el Centro de operaciones ni en la interfaz de línea de mandatos de administración. Se efectúa una copia de seguridad de los propios datos que se pueden restaurar correctamente pero el nombre del espacio de archivos o del archivo puede visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está activado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El resultado de la conversión de caracteres que no soporta la página de códigos actual depende del sistema operativo. Los nombres que IBM Spectrum Protect puede convertir parcialmente pueden ir acompañados de signos de interrogación (??), espacios en blanco, caracteres que no se pueden imprimir o "...". Estos caracteres indican al administrador que existen archivos. Si la conversión no es satisfactoria, el nombre se visualiza como "...". La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.




Un nombre de archivo visualizado como "....." indica que ni la ruta del archivo ni el nombre del archivo se han convertido correctamente. Un ejemplo de ruta y nombre puede ser:

```
my\dir\...
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY BACKUPSETCONTENTS

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)

Utilice este mandato para visualizar información acerca de los archivos dañados identificados durante un proceso de conversión de agrupación de almacenamiento.

Si emite el mandato CONVERT STGPOOL para convertir una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio, es posible que algunos archivos de la agrupación de almacenamiento de origen no se conviertan debido a los datos dañados. Para visualizar los datos dañados identificados durante el proceso de conversión, emita el mandato QUERY CLEANUP en una agrupación de almacenamiento de origen.

Para recuperar una versión sin daños de los datos de una agrupación de almacenamiento de copia o de datos activos, emita el mandato RESTORE STGPOOL. Para recuperar una versión sin daños de los datos de un servidor de réplica de destino, emita el mandato REPLICATE NODE y especifique el parámetro RECOVERDAMAGED=YES.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

Sintaxis

```
>>-Query CLeanup--nombre_agrupación-----><
```

Parámetros

nombre_agrupación (Obligatorio)
Especifica la agrupación de almacenamiento que se consulta.

Ejemplo: Visualizar los archivos dañados identificados por un proceso de conversión de agrupación de almacenamiento

Visualice los archivos dañados de una agrupación de almacenamiento denominada POOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query cleanup pool1

Nombre de archivo: \RTC\BDAT\GIGFILES\BF1.GB
Estado: Activo
Tamaño almacenado: 1 GB
Nombre de espacio de archivos: \\ibm838-r90gf0gx\c$
Tipo: Backup
Nombre de cliente: CAKINProtection
Fecha de protección: 03/25/2016 16:47:57
```

Descripciones de los campos

Nombre de archivo
El nombre del archivo dañado.

Estado
El estado de los datos en el inventario. Son posibles los siguientes estados:

Activo
La versión del archivo en el inventario está activa. Solo puede haber una versión activa del archivo en el inventario.

Inactivo
La versión del archivo en el inventario está inactiva. Pueden haber varias versiones inactivas del archivo en el inventario.

Tamaño almacenado
El tamaño de los datos, en megabytes (MB) o gigabytes (GB), que se almacenan en la agrupación de almacenamiento.

Nombre de espacio de archivos
El nombre del espacio de archivos donde está asignado el archivo.

Tipo
El tipo de operación utilizado para almacenar el archivo. Son posibles los valores siguientes:

Copia de seguridad
Archivos de los que se ha realizado una copia de seguridad.

Archivado
Archivos que se han archivado.

Gestión espacio
Archivos que se migran desde un cliente IBM Spectrum Protect for Space Management.

Nombre cliente
El nombre del cliente que es propietario del archivo.

Fecha de protección
Fecha y hora de la copia de seguridad, el archivado o la migración del archivo por parte del cliente de IBM Spectrum Protect for Space Management.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY CLEANUP

Mandato	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY CONVERSION	Consultar estado de conversión de una agrupación de almacenamiento.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.

QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)

Utilice este mandato para consultar un conjunto de opciones de cliente.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----.  
>>-Query CLOptset--+----->  
      '-nombre_conjunto_opciones-'  
  
>--+-----<<  
      '-DESCRiption----descripción-'
```

Parámetros

nombre_conjunto_opciones
Especifica el nombre del conjunto de opciones de cliente que se ha de consultar. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son los nombres de conjuntos de opciones.

DESCRiption
Especifica la descripción utilizada en los mandatos DEFINE o UPDATE CLOPTSET que debe utilizarse como filtro. Si la descripción contiene espacios, debe delimitarla con comillas. Este parámetro es opcional.

Ejemplo: consultar un conjunto de opciones de cliente

Desde un servidor gestionado, consultar el conjunto de opciones de cliente denominado ENG. Emita el mandato siguiente:

```
query cloptset eng

      Conjunto opciones: ENG
      Descripción:
Última actualización por (administrador): $$CONFIG_MANAGER$$
      Perfil de gestión:
      Replica Option Set: Yes

      Opción: SCROLLINES
      Número secuencia: 0
      Utilizar valor conjunto opciones (FORCE): No
      Valor opción: 40

      Opción: SCROLLPROMPT
      Número secuencia: 0
      Utilizar valor conjunto opciones (FORCE): No
      Valor opción: yes
```

Descripciones de los campos

Conjunto de opciones

Especifica el nombre del conjunto de opciones.

Descripción

Especifica la descripción del conjunto de opciones de cliente.

Última actualización por (administrador)

Especifica el nombre del administrador que ha actualizado por última vez el conjunto de opciones. Si este campo contiene \$\$CONFIG_MANAGER\$\$, el conjunto de opciones de cliente está asociado a un perfil que gestiona el gestor de configuración.

Perfil de gestión

Especifica el perfil en el que se ha inscrito el servidor gestionado para obtener la definición de este conjunto de opciones de cliente.

Opción de réplica

Especifica que el conjunto de opciones de réplica lo replica el servidor de réplica de origen.

Opción

Especifica el nombre de la opción.

Número de secuencia

Especifica el número de secuencia de la opción.

Utilizar valor de conjunto de opciones (FORCE)

Especifica si el valor de la opción del servidor prevalece sobre el valor de la opción del cliente. NO indica que el valor de la opción del servidor no prevalece sobre el valor de la opción del cliente. YES indica que el valor de la opción del servidor prevalece sobre el valor de la opción del cliente. Esta opción se establece con el parámetro FORCE en el mandato DEFINE CLIENTOPT.

Valor de opción

Especifica el valor de la opción.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY CLOPTSET

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.

QUERY COLLOGROUP (Consultar un grupo de proximidad)

Utilice este mandato para visualizar los grupos de proximidad definidos en el servidor.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----.  
>>-Query COLLOGroup--+----->  
      '-nombre_grupo-'  
  
.Format----Standard----.  
>--+-----+----->>  
      '-Format----+Standard-+-'  
      '-Detailed-'
```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad que se visualizará. Para especificar varios nombres, utilice un carácter comodín. Este parámetro es opcional. El valor predeterminado es visualizar todos los grupos de proximidad.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información. Para visualizar los miembros del grupo de proximidad, debe especificar FORMAT=DETAILED.

Visualizar grupos de proximidad definidos

Mostrar los grupos de proximidad definidos en el servidor. Emita el mandato siguiente:

```
query collogroup
```

Nombre del grupo de proximidad	Descripción del grupo de proximidad
DEPT_ED	Departamento de formación
GROUP1	Nodos cliente de baja capacidad.

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Mostrar información detallada para grupos de proximidad

Mostrar información completa sobre todos los grupos de proximidad y determinar qué nodos cliente pertenecen a qué grupos de proximidad. Emita el mandato siguiente:

```
query collogroup format=detailed
```

```
Nombre del grupo de proximidad: DEPT_ED  
Descripción del grupo de proximidad: Departamento de formación  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora de la última actualización: 21/04/2013 10:59:03  
Miembro(s) del grupo de proximidad: EDU_1 EDU_7  
Miembros(s) de espacio de archivos:  
  
Nombre del grupo de proximidad: GROUP1_ED  
Descripción del grupo de proximidad: nodos cliente de baja  
capacidad.  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora de la última actualización: 21/04/2013 10:59:16
```

Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: alpha

Nombre del grupo de proximidad: GROUP1_ED
Descripción del grupo de proximidad: nodos cliente de baja capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:16
Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: beta

Nombre del grupo de proximidad: GROUP1_ED
Descripción del grupo de proximidad: nodos cliente de baja capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:16
Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: gamma

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de grupo de proximidad

El nombre del grupo de proximidad.

Descripción de grupo de proximidad

La descripción del grupo de proximidad.

Última actualización por (administrador)

El nombre del administrador que ha definido o ha actualizado más recientemente el grupo de proximidad.

Fecha/hora última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente el grupo de proximidad.

Miembro(s) de grupo de proximidad

Los miembros del grupo de proximidad.

Miembro(s) de espacio de archivos




El espacio o espacios de archivos miembros del grupo de proximidad. Si hay más de un espacio de archivos, aparecen cada uno en una entrada distinta.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY COLLOGROUP

Mandato	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.

Mandato	Descripción
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY CONTAINER (Consulta de un contenedor)

Utilice este mandato para visualizar información sobre uno o más contenedores.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query CONTAINER-+-----+----->
                    .-*-----
                    '-nombre_contenedor-'

>+-----+----->
  '-STGpool----nombre_agrupación-'

  .-Format----Standard----.  .-State----ANY-----
>+-----+-----+-----+----->
  '-Format----+Standard+-'  '-State----+AVailable---+'
      '-Detailed-'          +-UNAvailable-+
                          +-ANY-----+
                          +-REAdonly----+
                          '-PENding----'

  .-TYPe----ANY-----
>+-----+-----><
  '-TYPe----+NONdedup+-'
      +-DEDup----+
      +-CLOud----+
      '-ANY-----'

```

Parámetros

nombre_contenedor

Especifica el nombre del contenedor. Especifique uno de los siguientes valores:

*

Especifica que un asterisco (*) representa un carácter comodín. Utilice los caracteres comodín como, por ejemplo, un asterisco para que coincida con cualquier carácter. De forma alternativa, puede utilizar un signo de interrogación (?) o un signo de porcentaje (%) para hacer coincidir con exactitud un carácter. Si especifica un asterisco, se visualizarán todos los nombres de contenedor. Este es el valor predeterminado.

nombre_contenedor

Especifica el nombre del contenedor. La longitud máxima del nombre de archivo es de 1024.

STGpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. La longitud máxima del nombre de la agrupación de almacenamiento es de 30.

Format

Especifica el nivel de detalla de los resultados de la consulta. Este parámetro es opcional. Especifique uno de los siguientes valores:

Standard

Especifica que se visualiza un resumen de la información. Este es el valor predeterminado.

Detailed

Especifica que se visualizará información detallada.

STate

Especifica el estado del contenedor que se está consultando. Este parámetro es opcional. Especifique uno de los siguientes valores:

AVAIlable

Especifica que sólo se muestran los contenedores que están disponibles.

UNAIvailable

Especifica que sólo se muestran los contenedores que no están disponibles. Por ejemplo, un contenedor puede no estar disponible si la cabecera está dañada o si el contenedor no puede abrirse.

ANY

Especifica que se visualizan contenedores que se hallan en cualquier estado. Este es el valor predeterminado.

REAdonly

Especifica que sólo se visualizan contenedores cuyo estado es de sólo lectura. Los datos se pueden leer pero no se pueden grabar en el contenedor.

PENding

Especifica que sólo se visualizan contenedores cuyo estado es pendiente.

TYPE

Especifica el tipo de contenedor que se consulta. Este parámetro es opcional. Especifique uno de los valores siguientes:

NONdedup

Visualiza contenedores que contienen datos de los que no se eliminan duplicados. Este tipo de datos incluye metadatos, datos cifrados y datos que son demasiado pequeños para eliminar duplicados de datos.

DEDup

Visualiza contenedores que contienen datos con duplicados eliminados.

CLOud

Muestra los contenedores que están almacenados en una agrupación de almacenamiento en la nube.

ANY

Visualiza cualquier tipo de contenedor. Este es el valor predeterminado.

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: visualizar información sobre un contenedor

Consulte Descripciones de los campos para ver una descripción de los campos.

```
query container /Containers/09/0000000000000943.ncf
```

Container	Storage Pool Name	Container Type	State
/Containers/09/0000000000000943.ncf	STGPOOL1	Non Dedup	Available

 Sistemas operativos Windows

Ejemplo: visualizar información sobre un contenedor

Consulte Descripciones de los campos para ver una descripción de los campos.

```
query container C:\abc\00\0000000000000005.ncf
```

Container	Storage Pool Name	Container Type	State
C:\abc\00\0000000000000005.ncf	STGPOOL1	Non Dedup	Available

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: visualizar información detallada sobre un contenedor

Visualice información detallada sobre contenedores que contienen datos con duplicados eliminados en la agrupación de almacenamiento STGPOOL1:

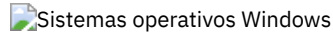
```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```

Container: /abc/00/0000000000000001.dcf
Nombre de la agrupación de almacenamiento: STGPOOL1
Tipo de contenedor: Dedup
Estado: Disponible
Tamaño máximo (MB): 40.960
Espacio libre (MB): 39.700
Fecha aprox. última grabación: 11/10/2014 15:17:09
Fecha aprox. de última auditoría:
Tipo de nube:

```

URL de nube:
Tamaño del objeto de nube (MB):
Espacio utilizado (MB):
Recuento de la extensión de datos:



Ejemplo: visualizar información detallada sobre un contenedor

Visualice información detallada sobre contenedores que contienen datos con duplicados eliminados en la agrupación de almacenamiento STGPOOL1:

```
query container stgpool=STGPOOL1 type=dedup format=detail

Container: C:\abc\00\0000000000000001.dcf
Nombre de la agrupación de almacenamiento: STGPOOL1
Tipo de contenedor: Dedup
Estado: Disponible
Tamaño máximo (MB): 40.960
Espacio libre (MB): 39.700
Fecha aprox. última grabación: 11/10/2014 15:17:09
Fecha aprox. de última auditoría:
Tipo de nube:
URL de nube:
Tamaño del objeto de nube (MB):
Espacio utilizado (MB):
Recuento de la extensión de datos:
```

Ejemplo: visualizar información detallada sobre los contenedores que están almacenados en una agrupación de almacenamiento en la nube

Visualice información detallada sobre los contenedores que están almacenados en la agrupación de almacenamiento en la nube CLOUDPOOL:

```
query container stgpool=CLOUDPOOL format=detail

Container: 7-64a1261000c811e58e8f005056c00008
Nombre agrupación almacenamiento: CLOUDPOOL
Container Type: Cloud
Estado:
Espacio libre (MB):
Tamaño máximo (MB):
Fecha aprox. última grabación: 05/22/2015 14:36:57
Fecha aprox. de última auditoría:
Tipo de nube: SWIFT
URL de nube: http://cloudurl:5000/v2.0
Tamaño del objeto de nube (MB):
Espacio utilizado (MB): 27
Recuento de la extensión de datos: 95
```

Descripciones de los campos

Contenedor

El nombre del contenedor.

Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

Tipo de contenedor

Tipo del contenedor.

Estado

El estado de los datos en el contenedor. El campo puede contener uno de los siguientes valores:

Disponible

El contenedor está disponible para su uso.

Unavailable

El contenedor no se puede abrir o validar.

Consejo: Emita el mandato `AUDIT CONTAINER` para validar el contenido del contenedor.

Sólo lectura

El contenedor puede leerse pero no se pueden escribir datos en el contenedor.

Pendiente

El contenedor está pendiente de supresión. Cuando caduca el valor especificado para el parámetro REUSEDELAY en el mandato DEFINE STGPOOL o UPDATE STGPOOL, el contenedor se suprime.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Tamaño máximo (MB)

El tamaño máximo del contenedor, en megabytes.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Espacio libre (MB)

La cantidad total de espacio libre que está disponible en el contenedor, en megabytes.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Fecha aprox. última grabación

La fecha y hora aproximadas en que se grabaron los datos en el contenedor.

Fecha aprox. de última auditoría

La fecha y hora aproximadas en que los datos se auditaron en el contenedor.

Tipo de nube

Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es el tipo de plataforma de la nube.

URL de nube

Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es el URL para acceder a la nube privada en las instalaciones o a la nube pública fuera de las instalaciones.

Tamaño de objeto de nube (MB)

El tamaño del objeto de nube, en megabytes, si el contenedor está representado por un objeto único en la agrupación de almacenamiento de contenedores en la nube.

Espacio utilizado (MB)

Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es la cantidad de espacio que utiliza el contenedor en la nube privada en las instalaciones o en la nube pública fuera de las instalaciones.

Recuento de extensiones de datos

Si el contenedor se almacena en una agrupación de almacenamiento de contenedor en la nube, es el número de extensiones de datos gestionadas por la nube privada en las instalaciones o la nube pública fuera de las instalaciones del contenedor.

Tabla 1. Mandatos relacionados con QUERY CONTAINER

Mandato	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
MOVE CONTAINER	Mueve el contenido de un contenedor de agrupación de almacenamiento a otro contenedor.
QUERY DAMAGED	Muestra información sobre los archivos dañados.

QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)

Utilice este mandato para visualizar la información sobre los archivos de un volumen de agrupación de almacenamiento y los nombres de archivos de cliente que se enlazan a un grupo con duplicados eliminados.

Puede utilizar este mandato para identificar los archivos que el servidor ha encontrado dañados y los archivos de los que se ha realizado una copia de seguridad en una agrupación de almacenamiento de copias o se han copiado en una agrupación de datos activos. Este mandato es útil cuando se daña un volumen o antes de que el usuario:

- Solicite al servidor que solucione las incoherencias entre un volumen y la base de datos
- Mueva archivos de un volumen a otro
- Suprima un volumen de una agrupación de almacenamiento

Puesto que este mandato puede tardar mucho tiempo en ejecutarse y los resultados pueden ser voluminosos, considere la posibilidad de utilizar el parámetro COUNT para limitar el número de archivos visualizados.

Nota: Los archivos que se almacenan en caché de un volumen de disco y que están marcados como dañados no se incluyen en el resultado.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query Content--nombre_volumen--+-----+----->
                                     '-NODE--==--nombre_nodo-'
>--+-----+----->
   '-Filespace--==--nombre_espacio_archivos-'
                                     .-Type--==--ANY-----
>--+-----+-----+-----+----->
   '-COUnt--==--número-'   '-Type--==--ANY-----'
                                     +-Backup-----+
                                     +-Archive-----+
                                     '-SPacemanaged-'
                                     .-Format----Standard----.   .-DAmaged--==--ANY-----
>--+-----+-----+-----+----->
   '-Format----+Standard-+-'   '-DAmaged--==--ANY-+-'
                                     '-Detailed-'           +-Yes-+
                                     +-No--'                 '-No--'
                                     (1)
   .-COPIed-----==--ANY-.   .-NAMEType--==--SERVER-----
>--+-----+-----+-----+----->
   '-COPIed-----+ANY-+-'   '-NAMEType--==--SERVER-+-'
                                     +-Yes-+           +-Unicode-+
                                     '-No--'           '-FSID----'
   .-CODEType--==--BOTH-----
>--+-----+----->
   '-CODEType--==--Unicode-----'
                                     +-NONUnicode-+
                                     '-BOTH-----'
   .-FOLLOWLinks--==--No-----
>--+-----+-----+-----><
   '-FOLLOWLinks--==--No-----+'
                                     +-Yes-----+
                                     '-JUSTLinks-'
```

Notas:

1. Utilice este parámetro únicamente para los volúmenes de las agrupaciones de almacenamiento primarias.

Parámetros

nombre_volumen (Necesario)

Especifica el volumen que se ha de consultar.

NODE

Especifica el cliente de copia de seguridad/archivado o de IBM Spectrum Protect for Space Management asociado al espacio de archivos que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica ningún nombre, se incluyen todos los clientes de copia de seguridad/archivado y IBM Spectrum Protect for Space Management.

Filespace

Especifica el espacio de archivos que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Si no especifica un nombre de espacio de archivos, se incluirán todos los espacios de archivos.

Para un servidor que tenga clientes con soporte de Unicode, es posible que necesite hacer que el servidor convierta el nombre de espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para obtener información detallada. Si no especifica ningún nombre de espacio de archivos o especifica sólo un carácter comodín para dicho nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

COUnt

Especifica el número de archivos que se han de visualizar. Este parámetro es opcional. Puede especificar un número entero negativo o un número entero positivo. Si especifica un número entero positivo, *n*, se visualizarán los *n* primeros archivos. Si especifica un número entero negativo, *-n*, se visualizarán los *n* últimos archivos en orden *inverso*. No es posible especificar COUNT=0. Si no especifica un valor para este parámetro, se visualizarán todos los archivos.

Type

Especifica los tipos de archivos que se consultan. Este parámetro es opcional. El valor predeterminado es ANY. Si el volumen que se consulta está asignado a una agrupación de datos activos, los únicos valores válidos son ANY y BACKUP. Los valores posibles son:

ANY

Especifica que se consultan todos los tipos de archivos del volumen de agrupación de almacenamiento; versiones de copia de seguridad de archivos, copias archivadas de archivos y archivos que clientes de IBM Spectrum Protect for Space Management migran desde los nodos cliente.

Backup

Especifica que sólo se consultarán los archivos de copia de seguridad.

Archive

Especifica que sólo se consultarán las copias archivadas. Este valor no es válido para las agrupaciones de datos activos.

SPacemanaged

Especifica que solo se consultan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management). Este valor no es válido para las agrupaciones de datos activos.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial. Los nombres Unicode se convierten a la página de códigos del servidor.

Detailed

Especifica que se visualizará toda la información. Los nombres Unicode se visualizan en formato hexadecimal.

DAMaged

Especifica criterios para restringir la salida de la consulta en función de si los archivos están marcados como dañados. A los efectos de estos criterios, el servidor sólo examina los archivos físicos (un archivo que puede ser un único archivo lógico o un añadido que consta de archivos lógicos). Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

ANY

Especifica que los archivos se visualizarán independientemente de si el servidor detectó que los archivos están dañados.

Yes

Especifica que sólo se visualizarán los archivos que están marcados como dañados. Son los archivos en los que el servidor ha detectado errores, cuando un usuario intentaba restaurar o recuperar el archivo o cuando se ejecutaba un mandato AUDIT VOLUME.

No

Especifica que sólo se visualizan los archivos que no se sabe si están dañados.

COPIed

Especifica los criterios para restringir la salida de la consulta en función de si la copia de seguridad de los archivos se ha hecho en una agrupación de almacenamiento de copia. El hecho que los archivos estén o no estén almacenados en una agrupación de datos activos no influye sobre el resultado. Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

ANY

Especifica que los archivos se visualizarán independientemente de si se ha realizado o no una copia de seguridad en una agrupación de almacenamiento de copia. Se visualizarán las copias de los archivos primarios y en caché.

Yes

Especifica que sólo se visualizarán los archivos de los que exista como mínimo una copia de seguridad utilizable en una agrupación de almacenamiento de copia. No se visualizará un archivo si se sabe que la copia que existe en la agrupación de almacenamiento de copia contiene errores. No se visualizarán las copias de archivos en caché ya que estos archivos no se restauran nunca.

Utilice COPIED=YES para identificar los archivos primarios que pueden restaurarse utilizando el mandato RESTORE VOLUME o RESTORE STGPOOL.

No

Especifica que sólo se visualizarán los archivos de los que no existan copias de seguridad utilizables en una agrupación de almacenamiento de copia. No se visualizarán las copias de archivos en caché ya que estos archivos no se restauran nunca.

Utilice COPIED=NO para identificar los archivos primarios que no pueden restaurarse utilizando el mandato RESTORE VOLUME o RESTORE STGPOOL.

NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Actualmente, un cliente de copia de seguridad/archivado con soporte Unicode sólo está disponible para Windows, Macintosh OS 9, Macintosh OS X y NetWare. Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado.

El valor predeterminado es SERVER. Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen los nombres y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

CODEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos.

El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Los valores posibles son:

UNICODE

Incluir los espacios de archivos que solo están en Unicode.

NONUNICODE

Incluir espacios de archivos que no están sólo en Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

FOLLOWLinks

Especifica si se mostrarán solo los archivos que están almacenados en el volumen o solo los archivos que están enlazados al volumen. También puede mostrar los archivos almacenados y los archivos enlazados. El valor predeterminado es NO. Los valores posibles son:

No

Se muestran solo los archivos que se encuentran almacenados en el volumen. No se muestran los archivos que tienen enlaces al volumen.

Yes

Se muestran todos los archivos, incluidos aquellos que están almacenados en el volumen y los que tienen enlaces al volumen.

JUSTLinks


Se muestran solo los archivos que tienen enlaces al volumen. No se muestran los archivos que están almacenados en el volumen.

Ejemplo: mostrar el contenido de un volumen para un nodo cliente específico

Consultar el contenido de un volumen y limitar el resultado a los archivos cuya copia de seguridad se hizo desde el nodo cliente PEGASUS.

 Sistemas operativos AIX  Sistemas operativos Linux Para el volumen /tsmstg/diskvol1.dsm, emita el mandato:

```
query content /tsmstg/diskvol1.dsm node=pegasus
type=backup
```

 Sistemas operativos Windows Para el volumen f:\tsmstg\diskvol1.dsm, emita el mandato:

```
query content f:\tsmstg\diskvol1.dsm node=pegasus
type=backup
```

El resultado del mandato incluye todos los archivos lógicos que forman cualquier agregación de archivos que hay en el volumen, incluso aunque la agregación de archivos esté almacenada en varios volúmenes además de éste. Con las agregaciones de archivos, la consulta no determina cuáles son los archivos lógicos que realmente están almacenados en el volumen cuya consulta se realiza.

zNombre nodo	Tipo	Espacio archivos	FSID	Nombre de archivo del cliente
PEGASUS	Bkup	\\pegasus\e\$	1	\UNI_TEST\ SM01.DAT
PEGASUS	Bkup	\\pegasus\e\$	1	\UNI_TEST\ SM02.DAT

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: mostrar información detallada para un volumen de cinta

Consultar el contenido del volumen de cinta denominado WPD001. Mostrar solo los archivos de los que ha realizado una copia de seguridad el nodo MARK y los archivos que están almacenados en el volumen o enlazados a él. Mostrar solo los cuatro primeros archivos del volumen.

```
query content wpd001 node=mark count=4 type=backup followlinks=yes
format=detailed
```

```

Nombre nodo: MARK
Tipo: C.S.
Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
FSID: 1
Nombre del archivo en el cliente: \UNI_TEST\ SM01.DAT
Nombre hexadecimal del archivo en el cliente:
¿Agregación?: 1/3
Tamaño almacenado: 2.746
Número de segmento:
¿Copia en caché?: No
Enlazado: No
Número de fragmento:

Nombre nodo: MARK
Tipo: C.S.
Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
FSID: 1
Nombre del archivo en el cliente: \UNI_TEST\ SM02.DAT
Nombre hexadecimal del archivo en el cliente:
¿Agregación?: 2/3
Tamaño almacenado: 2.746
Número de segmento:
¿Copia en caché?: No
Enlazado: No
Número de fragmento: 2

Nombre nodo: MARK
Tipo: C.S.
Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
FSID: 1
Nombre del archivo en el cliente: \UNI_TEST\ SM03.DAT
Nombre hexadecimal del archivo en el cliente:
¿Agregación?: 3/3
Tamaño almacenado: 2.746
Número de segmento:
¿Copia en caché?: No
Enlazado: No
Número de fragmento: 3
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Node Name

El nodo al que pertenece el archivo.

Type

Tipo de archivo: copia archivada (Arch), copia de seguridad (Bkup) o bajo gestión de espacio (SpMg) mediante un cliente IBM Spectrum Protect for Space Management.

Filespace Name

El espacio de archivos al que pertenece el archivo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre espacio archivos hexadecimal

El espacio de archivos al que pertenece el archivo. Si el nombre del espacio de archivos está en Unicode, el nombre se visualiza en formato hexadecimal.

FSID

El identificador del espacio de archivos (FSID). El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

Nombre del archivo en el cliente

El nombre del archivo en el cliente.

Los nombres de espacios de archivos y nombres de archivo que pueden estar en una página de códigos o un entorno local diferente de los del servidor no se visualizan correctamente en el Centro de operaciones ni en la interfaz de línea de mandatos de administración. Se efectúa una copia de seguridad de los propios datos que se pueden restaurar correctamente pero el nombre del espacio de archivos o del archivo puede visualizarse con una combinación de caracteres no válidos o espacios en blanco. El resultado de la conversión de caracteres que no soporta la página de códigos actual depende del sistema operativo. Los nombres que IBM Spectrum Protect puede convertir parcialmente pueden ir acompañados de signos de interrogación (??), espacios en blanco, caracteres que no se pueden imprimir o "...". Estos caracteres indican al administrador que existen archivos.

Nombre de cliente hexadecimal para archivo

El nombre del cliente del archivo que se visualiza en formato hexadecimal.

Aggregated?

Si el archivo es un archivo lógico que está almacenado como componente de una agregación de archivos. Si el archivo forma parte de una agregación de archivos, se visualizan la secuencia de este archivo en la agregación de archivos y el número total de archivos lógicos que hay en la agregación de archivos. El resultado del mandato incluye todos los archivos lógicos que forman cualquier agregación de archivos que hay en el volumen, incluso aunque la agregación de archivos esté almacenada en varios volúmenes además de éste. La consulta no determina cuáles son los archivos lógicos que realmente están almacenados en el volumen cuya consulta se realiza.

Si el archivo no forma parte de un agregado, el campo muestra "no".

Tamaño almacenado

El tamaño del archivo físico, en bytes. Si el archivo es un archivo lógico que está almacenado como componente de una agregación de archivos, este valor indica el tamaño de toda la agregación de archivos.

Número de segmento

En volúmenes de agrupaciones de almacenamiento de acceso secuencial, especifica si el archivo físico (tanto si es un único archivo lógico como si es una agregación de archivos lógicos) se almacena en varios volúmenes. Por ejemplo, si el archivo lógico se almacena en una agregación de archivos que abarca dos volúmenes, el número de segmento indica 1/2 (la primera parte del archivo físico se almacena en el volumen) o 2/2 (la segunda parte del archivo físico se almacena en el volumen). Si el número de segmento es 1/1, el archivo físico se almacena entero en el volumen. Para los volúmenes de las agrupaciones de almacenamiento de acceso aleatorio, no se visualiza ningún valor.

¿Copia en caché?

Si el archivo físico es una copia en caché de un archivo migrado a la siguiente agrupación de almacenamiento. Si el archivo forma parte de una agregación de archivos, este valor pertenece a la agregación de archivos.

Enlazado

Indica si el archivo se almacena en el volumen o si se encuentra enlazado al volumen.

Número de fragmento




Especifica el número de fragmento. Si el número de fragmento está en blanco, es el primer fragmento o no es un fragmento.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY CONTENT

Mandato	Descripción
---------	-------------

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)

Utilice este mandato para visualizar información acerca de una operación de conversión. Puede convertir una agrupación de almacenamiento primario que utiliza una clase de dispositivo de tipo FILE o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedor de directorios.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

Sintaxis

```
>>-Query CONVERSion--+-+-----+----->
                        '-nombre_agrupación-'
.-Format----Standard----.
>--+-+-----+-----<<
  '-Format--+-+Standard-+-'
                        '-Detailed-'
```

Parámetros

nombre_agrupación

Especifica la agrupación de almacenamiento que se consulta. Este parámetro es opcional. Si no especifica un valor para este parámetro, la información se visualiza para todas las agrupaciones de almacenamiento.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información de conversión para todas las agrupaciones de almacenamiento

Visualizar información de conversión para todas las agrupaciones de almacenamiento. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query conversion
```

Source Storage Pool	Target Storage Pool	Starting Amount	Total Converted	Last Converted
FILEPOOL	CTR	3 GB		3 GB
FPOOL	CTR	333 MB	333 MB	267 MB

Ejemplo: visualizar información detallada sobre la conversión de agrupación de almacenamiento

Visualizar información detallada sobre la conversión de agrupación de almacenamiento. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query conversion format=detailed

Agrupación de almacenamiento de origen: FILEPOOL
Agrupación de almacenamiento de destino: CTR
Número máximo de procesos: 4
Duración: 60 minutos
Cantidad inicial: 333 MB
Total convertido: 333 MB
Último convertido: 333 MB
Fecha/hora inicio: 03/24/2016 13:22:32
```

Descripciones de los campos

Agrupación de almacenamiento de origen

El nombre de la agrupación de almacenamiento que se está convirtiendo.

Agrupación de almacenamiento de destino

El nombre de la agrupación de almacenamiento de destino donde se almacenarán los datos convertidos.

Número máximo de procesos

Especifica el número máximo de procesos de conversión.

Duración

Especifica el tiempo, en minutos, para la conversión.

Cantidad inicial

La cantidad inicial de datos a convertir, en megabytes (MB), gigabytes (GB) o terabytes (TB).

Total convertido

La cantidad total de datos convertidos, en megabytes (MB), gigabytes (GB) o terabytes (TB).

Último convertido

La cantidad de datos, en megabytes (MB), gigabytes (GB) o terabytes (TB), convertidos durante este proceso de conversión.

Fecha/hora inicio

La fecha y la hora en que se emitió el mandato CONVERT STGPOOL por primera vez para la agrupación de almacenamiento.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY CONVERSION

Mandato	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.

QUERY COPYGROUP (Consultar grupos de copia)

Utilice este mandato para visualizar información sobre uno o varios grupos de copia.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query COpygroup----->
. -*--*--*--STANDARD-----
>--+-----+-->
```

```

| .-*--*--STANDARD-----|
'-nom_dominio-----|
| .-*--STANDARD-----|
'-nom_juego_políticas-----|
| .-STANDARD-. |
'-nom_clase-----|
'-STANDARD-'

.-Type---Backup----- .-Format---Standard-----
>-----<
'-Type---Backup---|'-Format---Standard-|
'-Archive-' '-Detailed-'

```

Parámetros

nombre_dominio

Especifica el dominio de políticas asociado al grupo de copia que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los dominios de políticas. Debe especificar este parámetro cuando consulte un grupo de copia denominado explícitamente.

nombre_juego_políticas

Especifica el juego de políticas asociado al grupo de copia que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los juegos de políticas. Debe especificar este parámetro cuando consulte un grupo de copia denominado explícitamente.

nombre_clase

Especifica la clase de gestión asociada al grupo de copia que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todas las clases de gestión. Debe especificar este parámetro cuando consulte un grupo de copia denominado explícitamente.

STANDARD

Especifica el nombre del grupo de copia. Este parámetro es opcional. El nombre del grupo de copia debe ser STANDARD. El valor predeterminado es STANDARD.

Type

Especifica el tipo del grupo de copia que se ha de consultar. Este parámetro es opcional. El valor predeterminado es BACKUP. Los valores posibles son:

Backup

Especifica que desea consultar los grupos de copia de seguridad.

Archive

Especifica que desea consultar los grupos de copia archivada.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información sobre el grupo de copia de seguridad predeterminado

Visualizar información sobre el grupo de copias de seguridad predeterminado en el dominio de políticas de ingeniería ENGPOLDOM. Emita el mandato siguiente:

```
query copygroup engpoldom * *
```

Los datos siguientes muestran la salida de la consulta. Muestra que el conjunto de políticas ACTIVE contiene dos grupos de copias que pertenecen a las clases de gestión MCENG y STANDARD.

Nombre Dominio	Nombre grupo nombre	Nombre clase nombre	Nombre grupo nombre	Versiones datos existen	Versiones datos suprimidos	Retener Extra	Retener sólo versiones
ENGPOLDOM	ACTIVE	MCENG	STANDARD	5	4	90	600
ENGPOLDOM	ACTIVE	STANDARD	STANDARD	2	1	30	60
ENGPOLDOM	STANDARD	MCENG	STANDARD	5	4	90	600
ENGPOLDOM	STANDARD	STANDARD	STANDARD	2	1	30	60
ENGPOLDOM	TEST	STANDARD	STANDARD	2	1	30	60

Ejemplo: mostrar información detallada acerca de un grupo de copias de seguridad

Mostrar información completa sobre grupo de copia de seguridad asignado a la clase de gestión ACTIVEFILES del juego de políticas VACATION, del dominio de políticas EMPLOYEE_RECORDS. Emita el mandato:

```
query copygroup employee_records vacation
activefiles format=detailed
```

Ejemplo: mostrar información acerca del grupo de copias de seguridad asignado en la clase de gestión y juego de políticas STANDARD

Desde un servidor gestionado, visualizar información completa sobre el grupo de copia de seguridad asignado a la clase de gestión STANDARD del juego de políticas STANDARD del dominio de políticas ADMIN_RECORDS. Emita el mandato:

```
query copygroup admin_records
standard standard format=detailed

Nombre dominio políticas: ADMIN_RECORDS
Nombre juego políticas: STANDARD
Nombre clase gestión: STANDARD
Nombre grupo copia: STANDARD
Tipo grupo de copia: Copia seguridad
Versiones si datos existen: 2
Versiones si datos suprimidos: 1
Retener versión adicional: 30
Retener única versión: 60
    Modalidad copia: Modificado
Serialización copia: Estático compartido
Frecuencia copias: 0
Destino copias: BACKUPOOL
Destino de Tabla de contenido (TOC):
    Última actualización por (administrador): $$CONFIG_MANAGER$$
    Fecha/Hora última actualización: 2002.10.02 17.51.49
    Perfil de gestión: ADMIN_INFO
    Cambios pendientes: Sí
```

Ejemplo: mostrar información acerca del grupo de copias archivadas

Desde un servidor gestionado, visualizar información completa sobre el grupo de copia archivada STANDARD que está asignado a la clase de gestión MCLASS1 del juego de políticas SUMMER del dominio de políticas PROG1. Emita el mandato:

```
query copygroup progl1 summer mclass1
type=archive format=detailed

Nombre dominio políticas: PROG1_RECORDS
Nombre juego políticas: SUMMER
Nombre clase gestión: MCLASS1
Nombre grupo copia: STANDARD
Tipo grupo copia: Archivado
Retener versión: 730
Iniciación de retención: Creación
Retención mínima:
Serialización copia: Estático compartido
Frecuencia copia: Cmd
    Modalidad copia: Absoluto
Destino copia: ARCHPOOL
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/Hora última actualización: 2002.10.02 17.42.49
Perfil de gestión: ADMIN_INFO
```

Ejemplo: mostrar información acerca del grupo de copias para una copia de seguridad NAS

Consultar al grupo de copias acerca de la copia de seguridad NAS. Emita el mandato:

```
query copygroup nasdomain
type=backup

Nombre dominio políticas: NASDOMAIN
Nombre juego políticas: ACTIVE
Nombre clase gestión: STANDARD
Nombre grupo copia: STANDARD
Tipo grupo de copia: Copia seguridad
Versiones si datos existen: 2
```

Versiones si datos suprimidos: 1
 Retener versión adicional: 30
 Retener única versión: 60
 Modalidad copia: Modificado
 Serialización copia: Estático compartido
 Frecuencia copias: 0
 Destino copias: NASPOOL
 Destino de tabla de contenido (TOC): BACKUPPOOL
 Última actualización por (administrador): SERVER_CONSOLE
 Fecha/Hora última actualización: 10/02/2002 12:16:52
 Perfil de gestión:
 Cambios pendientes: Sí

Descripciones de los campos




- Nombre de dominio de políticas**
El nombre del dominio de políticas.
- Nombre de juego de políticas**
El nombre del juego de políticas.
- Nombre clase gestión**
El nombre de la clase de gestión.
- Nombre grupo copia**
El nombre del grupo de copia. Este nombre siempre es STANDARD.
- Tipo grupo copia**
El tipo del grupo de copia.
- Versiones si datos existen**
Número máximo de versiones de copia de seguridad que han de retenerse para los archivos que actualmente se encuentran en el sistema de archivos del cliente.
- Versiones si datos suprimidos**
Número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad utilizando IBM Spectrum Protect.
- Retener versión adicional**
Número de días que ha de retenerse una versión de copia de seguridad cuando la versión pasa a ser inactiva.
- Retener única versión**
Número de días que ha de retenerse la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente.
- Serialización copias**
Si puede utilizarse un archivo durante una operación de archivado.
- Frecuencia copia**
La frecuencia de copias del grupo de copia. En los grupos de copia archivada, este valor siempre es CMD.
- Modalidad copia**
Especifica que los archivos del grupo de copia se archivan independientemente de si se han modificado. En los grupos de copia archivada, este valor siempre es ABSOLUTE.
- Destino de copia**
El nombre de la agrupación de almacenamiento donde el servidor almacena inicialmente los archivos asociados a este grupo de copia archivada.
- Destino de tabla de contenido (TOC)**
Nombre de la agrupación de almacenamiento primaria en la que inicialmente se almacenan las TOC para las operaciones de copia de seguridad de imagen en las que se solicita la generación de la TOC.
- Última actualización por (administrador)**
El nombre del administrador o del servidor que ha actualizado por última vez el grupo de copia. Si este campo contiene \$\$CONFIG_MANAGER\$\$, el grupo de copias está asociado a un dominio que gestiona el gestor de configuración.
- Fecha/hora última actualización**
La fecha y la hora en que se ha definido o actualizado por última vez el grupo de copia.
- Perfil de gestión**
El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este grupo de copias de políticas.
- Cambios pendientes**
Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY COPYGROUP

Mandato	Descripción
---------	-------------

Mandato	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)

Utilice este mandato para visualizar información sobre las extensiones de datos dañadas de una agrupación de almacenamiento de contenedores de directorios o de nubes. Utilice este mandato junto con el mandato AUDIT CONTAINER para determinar un método de recuperación para los datos dañados.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query DAMaged--nombre_agrupación----->>
. -Type----Status-----
>--+-----+-----+-----+-----><
'-Type----+-INventory-----+'
      +-Node--| A |-----+
      '-CONTAINER--| A |-'

A (filtro adicional por nombre de nodo)

|---+-----+-----+-----+-----|
  '-Nodename----nombre_nodo-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio o de nube.

Type

Especifica el tipo de información que desea visualizar. Este parámetro es opcional. Especifique uno de los siguientes valores:

Status

Especifica que se visualiza información sobre extensiones de datos dañadas. Para las agrupaciones de almacenamiento de nube, también se visualizan las extensiones huérfanas. Este es el valor predeterminado.

Nodo

Especifica que se visualiza información sobre el número de archivos dañados por nodo.

INventory

Especifica que se visualiza información de inventario para cada archivo dañado.

CONTAINER

Especifica que se visualizan los contenedores que contienen extensiones de datos dañadas o extensiones huérfanas en la nube. Para las agrupaciones de almacenamiento de contenedores de directorio, también se visualizan los directorios de agrupación de almacenamiento.

Nodename

Especifica que se visualiza la información del archivo dañado para un único nodo.

Restricción: No puede especificar este parámetro si se ha especificado el parámetro TYPE=CONTAINER o TYPE=STATUS.

Ejemplo: Visualizar información de estado sobre extensiones de datos dañadas o huérfanas

Visualizar información sobre el estado de las extensiones de datos dañadas que están almacenadas en un contenedor.

```
query damaged pool1 type=status
```

Agrup. de almac. Name	Datos de no dedup. Extent Count	Datos de dedup. Extent Count	Huérfano de nube Extent Count
POOL1	58	145	

Para las agrupaciones de almacenamiento en la nube, también se visualiza el número de extensiones huérfanas.

Agrup. de almac. almacenamiento	Datos de no dedup. sin duplic. eliminados	Datos de dedup. con duplic. eliminados	Huérfano de nube de nube huérfanas
POOL1	65	238	18

Ejemplo: visualizar información sobre un archivo dañado para un tipo de nodo

Visualice información sobre los archivos dañados que están almacenados en un nodo.

```
query damaged pool1 type=node
```

Node Name	Number of Damaged Files
POOL1	37

Ejemplo: visualizar información sobre un archivo dañado para un tipo de inventario

Visualice la información acerca de los archivos dañados almacenados en un inventario.

```
query damaged pool2 type=inventory
```

```
Nombre del archivo en el cliente: /data/files/10.out
Tipo: C.S.
Nombre nodo: NODE1
Nombre de espacio de archivos: /data/space
Estado: Disponible
Hora de inserción: 01/19/2015 16:01:35
ID de objeto: 2073
```

Ejemplo: visualizar información sobre un archivo dañado para un tipo de contenedor

Visualice información sobre los archivos dañados que están almacenados en un contenedor.

```
query damaged pool3 type=container
```

```
ID de directorio: 1
Directorio: /abc/space/container1
Contenedor: /abc/space/container1/00/000000000000022.dcf
Estado: No disponible
```

Para los contenedores en la nube, sólo se visualiza el nombre del contenedor.

```
ID de directorio:
Directorio:
Contenedor: ibmsp.12520ae05b4011e613320a0027000000/
001-10006a3278bc34f0e4118a850090fa3dcb48/
00000000000001.ncf
Estado:
```

Para el almacenamiento local, se muestra la información siguiente acerca de un contenedor dañado.

```
ID de directorio: 1
Directorio: localdirectory
Contenedor: localdirectory/00/00000000000011.ncf
Estado: No disponible
```

Descripciones de los campos

Nombre del archivo en el cliente (solo TYPE=INVENTORY)

El nombre del archivo.

Recuento de extensiones huérfanas en la nube (solo TYPE=STATUS)

El número de extensiones huérfanas en una agrupación de almacenamiento en la nube. Las extensiones son consideradas huérfanas si no tienen una entrada de base de datos correspondiente.

Contenedor (solo TYPE=CONTAINER)

El nombre del contenedor.

Recuento de extensiones con duplicados eliminados (solo TYPE=STATUS)

El número de extensiones dañadas en la agrupación de almacenamiento para datos duplicados eliminados.

Directorio (solo TYPE=CONTAINER)

El nombre del directorio de la agrupación de almacenamiento.

ID de directorio (solo TYPE=CONTAINER)

El número de identificación del directorio de agrupación de almacenamiento.

Nombre del espacio de archivos (solo TYPE=INVENTORY)

El nombre del espacio de archivos.

Hora de la inserción (solo TYPE=INVENTORY)

La fecha y la hora en las que el objeto se ha almacenado en el servidor.

Nombre de nodo (solo TYPE=INVENTORY o TYPE=NODE)

El nombre del nodo.

Recuento de extensiones sin duplicados eliminados (solo TYPE=STATUS)

El número de extensiones dañadas en la agrupación de almacenamiento para datos que no son duplicados eliminados, como metadatos y datos cifrados de cliente.

Número de archivos dañados (solo TYPE=NODE)

El número de archivos dañados por nodo.

ID de objeto (solo TYPE=INVENTORY)

El número de identificación del objeto.

Estado (solo TYPE=INVENTORY o TYPE=CONTAINER)

El estado de los datos en el inventario o el contenedor, en función del tipo de datos que esté consultando. El campo puede contener uno de los siguientes valores:

Activo

La versión del archivo en el inventario está activa. Sólo puede haber una versión activa del archivo en el inventario.

Inactivo

La versión del archivo en el inventario está inactiva. Puede haber varias versiones inactivas del archivo en el inventario.

Disponible

El estado del contenedor es disponible.

No disponible

El estado del contenedor es no disponible. Por ejemplo, un contenedor puede no estar disponible si la cabecera está dañada o si el contenedor no puede abrirse.

Sólo lectura

El contenedor está en estado de solo lectura. Los datos del contenedor se pueden leer pero no se pueden grabar en el contenedor.

Pendiente

El contenedor está pendiente de supresión. El contenido del contenedor se ha trasladado a un contenedor diferente y el contenedor está listo para ser suprimido.

Tipo (solo TYPE=INVENTORY)

El tipo de datos del archivo.

Tabla 1. Mandatos relacionados con QUERY DAMAGED

Mandato	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.
QUERY CONTAINER	Visualiza información sobre un contenedor.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.

QUERY DATAMOVER (visualizar definiciones de un transportador de datos)

Utilice este mandato para visualizar definiciones de transportadores de datos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----  
>>-Query DATAMover----->  
      '-nombre_transportador_datos-'  
  
.Format----Standard----  
>----->  
      '-Format----Standard-+'  
      '-Detailed-'  
  
.Type-----*-----  
>-----<  
      |                               (1) (2) |  
      '-Type----+-NAS-----+'  
      +-NASCLUSTER-+  
      '-NASVSERVER-'
```

Notas:

1. Debe especificar el parámetro TYPE si `FORMAT=DETAILED`.
2. Puede especificar `TYPE=NASCLUSTER` y `TYPE=NASVSERVER` solo en un sistema operativo AIX, Linux o Windows.

Parámetros

nombre_transportador_datos

Especifica el nombre del transportador de datos que se visualizará. Puede especificar varios nombres con un carácter comodín. De forma predeterminada, se visualizarán todos los transportadores de datos.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD.

Standard

Especifica que se visualizará la información de nombre y dirección.

Detailed

Especifica que se visualizará toda la información.

Type

Especifica el tipo de transportador de datos que se visualizará. Si especifica `FORMAT=DETAILED`, debe especificar un valor para el parámetro TYPE.

NAS

Especifica un servidor de archivos de NAS.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NASCLUSTER

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica un servidor de archivos NAS en clúster.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NASVSERVER

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica un dispositivo de almacenamiento virtual dentro de un clúster.

Ejemplo: visualizar información acerca de todos los transportadores de datos

Visualizar los transportadores de datos en el servidor. Emita el mandato:

```
query datamover
```

```
Nombre de  
transportador de datos   Tipo de transportador de datos   En línea  
-----
```

NASMOVER1	NAS	Sí
NASMOVER2	NAS	No

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información acerca de un transportador de datos

Visualice información parcial sobre el transportador de datos DATAMOVER6. Emita el mandato:

```
query datamover datamover6 type=nas

Nombre origen      Tipo      Activado
-----
DATAMOVER6        NAS      Sí
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.




Ejemplo: visualizar información detallada acerca de un transportador de datos

Visualice información detallada sobre el transportador de datos DATAMOVER6. El parámetro TYPE es necesario si FORMAT = DETAILED. Emita el mandato:

```
query datamover datamover6 format=detailed type=nas

Nombre de transportador de datos: DataMover6
Tipo de transportador de datos:   NAS
Dirección IP: 198.51.100.0
Número de puerto TCP/IP: 10000
Nombre de usuario: NDMPadmin
Formato datos agrupación almacenamiento: NDMPDUMP
Activado: Yes
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 05/23/2015 09:26:33
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: visualizar información detallada acerca de un transportador de datos NAS en clúster

Visualice información detallada acerca de un transportador de datos NAS en clúster de nombre CLUSTERA Emita el mandato siguiente:

```
query datamover clustera format=detailed type=nascluster

Nombre de transportador de datos: CLUSTERA
Tipo de transportador de datos: NASCLUSTER
Dirección IP: 192.0.2.255
Número de puerto TCP/IP: 10000
Nombre de usuario: ndmp
Formato de datos de agrupación de almacenamiento: NETAPPDUMP
Activado: Yes
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 04/28/2015 09:26:33
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de transportador de datos

Especifica el nombre del transportador de datos.

Tipo de transportador de datos

Especifica el tipo de transportador de datos.

Dirección IP

Especifica la dirección IP del transportador de datos.

Número de puerto TCP/IP

Especifica el número de puerto TCP del transportador de datos.

Nombre usuario

Especifica el ID de usuario que utiliza el servidor para obtener acceso al transportador de datos.

Formato de datos de agrupación de almacenamiento

Especifica el formato de datos utilizado por el transportador de datos.

Activado

Especifica si el transportador de datos está en línea y disponible para utilizarlo.

Última actualización por (administrador)

Especifica el ID del administrador que ha realizado la última actualización.

Fecha/hora última actualización

Especifica la fecha y hora de la última actualización.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DATAMOVER

Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DELETE DATAMOVER	Suprimir un transportador de datos.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

QUERY DB (Visualizar información de base de datos)

Utilice este mandato para visualizar información sobre la base de datos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-Format----Standard----.
>>-Query DB-----+-----+-----<<
      '-Format---+-Standard+-'
              '-Detailed-'
```

Parámetros

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar estadísticas de resumen acerca de la base de datos

Visualiza información de estadísticas acerca de la base de datos. Emita el mandato:

```
query db
```

```
Base datos  Total pág.  Pág. utilizables  Pág. utiliz.  Pág. libres
-----
      TSMDB1      32.776      32.504      24.220      8.284
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información detallada de la base de datos

Visualizar información estadística detallada acerca de la base de datos. Emita el mandato:

```
query db format=detailed
```

```
Nombre de la base de datos: TSM_DB2
Espacio total del sistema de archivos (MB): 1.748.800
Espacio utilizado del sistema de archivos (MB): 2,304,355
Espacio utilizado por la base de datos (MB): 448
Espacio libre disponible (MB): 235.609
```



Páginas en total: 32.776
Páginas utilizables: 32.504
Páginas utilizadas: 24.220
Páginas libres: 8.284
Proporción aciertos agrupación búferes: 99,3
Total peticiones búferes: 204.121
Clasificar desbordamientos: 0
Proporción aciertos caché paquete: 89,8
Última reorganización base datos: 05/25/2009 16:44:06
Nombre completo clase dispositivo: FILE
Número de corrientes de copia de seguridad de base de datos: 4
Incrementales desde última completa: 0
Fecha/hora última copia seguridad completa: 05/18/2009 22:55:19
Comprimir copias de seguridad de base de datos: Sí
Proteger clave de cifrado maestra: No



Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.


Descripciones de los campos


Nombre de la base de datos

Nombre de la base de datos que se ha definido y configurado para que la utilice el servidor IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux Espacio total del sistema de archivos (MB)

 Sistemas operativos AIX  Sistemas operativos Linux El espacio total, en megabytes, del sistema de archivos en el que se encuentra la base de datos.

 Sistemas operativos Windows Espacio total del sistema de archivos (MB)

 Sistemas operativos Windows El espacio total, en megabytes, de las unidades en las que se encuentra la base de datos.

Espacio utilizado en el sistema de archivos (MB)

Cantidad de espacio de base de datos, en megabytes, que se utiliza.

Espacio utilizado por la base de datos (MB)

Especifica el tamaño de la base de datos en megabytes. El valor no incluye ningún espacio de tabla temporal. El tamaño de la base de datos se calcula a partir de la cantidad de espacio utilizado en el sistema de archivos que contiene la base de datos.

Espacio libre disponible (MB)

Cantidad de espacio de base de datos, en megabytes, que no se utiliza.

Páginas en total

El número total de páginas en el espacio de tabla.

Páginas utilizables

El número de páginas utilizables en el espacio de tabla.

Páginas utilizadas

El número de páginas utilizadas en el espacio de tabla.

Páginas libres

El número total de páginas libres en todos los espacios de tabla. La base de datos de IBM Spectrum Protect tiene un máximo de 10 espacios de tabla.

Proporción aciertos agrupación búferes

Porcentaje total de proporción de aciertos.

Total peticiones búferes

Número total de lecturas lógicas de datos de agrupación de búferes y de lecturas lógicas de índice desde la última vez que se inició la base de datos o desde que se restableció el supervisor de base de datos.

Clasificar desbordamientos

Número total de clasificaciones que se han quedado sin almacenamiento dinámico de clasificación y que pueden necesitar espacio de disco para almacenamiento temporal.

Proporción de aciertos de caché de paquete

Porcentaje que indica la capacidad de ayuda de la caché de paquete para evitar la recarga de paquetes y secciones para SQL estático desde los catálogos del sistema. También indica la capacidad de ayuda de la caché de paquete para evitar la recompilación de las sentencias SQL dinámicas. Una proporción alta indica el éxito en evitar estas actividades.

Última reorganización base datos

Última vez que el gestor de bases de datos ha completado una actividad de reorganización automática.

Nombre completo clase dispositivo

Nombre de la clase de dispositivo que se utiliza para las copias de seguridad completas de la base de datos.

Número de corrientes de copia de seguridad de base de datos

El número de corrientes de movimiento de datos simultáneas que se han utilizado durante la copia de seguridad de la base de datos.

Incrementales desde última completa

Número de copias de seguridad incrementales que se han completado desde la última copia de seguridad completa.

Fecha/hora última copia seguridad completa

La fecha y hora de la última copia de seguridad completa.

Comprimir copias de seguridad de base de datos

Especifica si las copias de seguridad de base de datos se comprimen.
Proteger clave de cifrado maestra

Especifica si las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DB

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)

Utilice este mandato para mostrar la información sobre los directorios que utiliza la base de datos para almacenar los datos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-QUERY DBSpace-----<<
```

Parámetros

Ninguno.

Ejemplo: visualizar información de espacio de almacenamiento de base de datos

Visualizar información acerca del espacio de almacenamiento de la base de datos. Emita el mandato:

```
query dbspace
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ubicación	Espacio total del sistema de archivos (MB)	Espacio utilizado en el sistema de archivos (MB)	Espacio libre disponible (MB)
/tsmdb001 117.804,422	1.748.800	1.513.191,125	
/tsmdb002 117.804,422	1.748.800	1.513.191,125	

 Sistemas operativos Windows

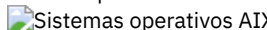
Ubicación	Espacio total de sistema de archivos (MB)	Espacio utilizado sistema de archivos (MB)	Espacio libre disponible (MB)
d:\tsm\db001	1.748.800	1.513.191,125	117.804,422
e:\tsm\db002	1.748.800	1.513.191,125	117.804,422


Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos


Ubicación

Especifica las ubicaciones de los directorios de base de datos.

 Sistemas operativos AIXEspacio total del sistema de archivos (MB)



 Sistemas operativos AIX La cantidad total de espacio, en megabytes, del sistema de archivos en el cual se encuentra la base de datos.


 Sistemas operativos Windows Espacio total del sistema de archivos (MB)

 Sistemas operativos Windows La cantidad total de espacio, en megabytes, de las unidades en las cuales se encuentra la base de datos.

Espacio utilizado en sistema de archivos (MB)


La cantidad de espacio de almacenamiento, en megabytes, que se utiliza.


 Sistemas operativos AIX  Sistemas operativos Linux Cuando ejecuta el mandato QUERY DBSPACE, el valor en la salida podría ser mayor que el valor que se obtiene al ejecutar el mandato df system. La salida para el mandato df system no incluye la cantidad de espacio reservada para el usuario root.

 Sistemas operativos Linux Si ejecuta el mandato df system, el porcentaje predeterminado de espacio reservado para el usuario root es 5%. Puede cambiar este valor predeterminado.

Espacio libre disponible (MB)

Cantidad de espacio, en megabytes, que no se utiliza.




 Sistemas operativos Windows Espacio libre disponible (MB)

 Sistemas operativos Windows Cantidad de espacio que queda en la unidad en la que se encuentra el directorio.

Mandos relacionados

Tabla 1. Mandatos relacionados con QUERY DBSPACE

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DB	Visualiza información de asignación acerca de la base de datos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)

Utilice este mandato para visualizar información sobre estadísticas de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o una agrupación de almacenamiento de nube.

Debe emitir el mandato GENERATE DEDUPSTATS para poder emitir el mandato QUERY DEDUPSTATS.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query DEDUPStats+-----+-----+-----+----->
                    '-nombre_agrupación-' '-nombre_nodo-'

.-*-----
>+-----+-----+-----+----->
| .-,-----|
| V          | |
+---nombre_espacio_de_archivos+---+
| .-,-----|
| V          | |
'-----FSID-----'

.-Format----Standard----.
>+-----+-----+-----+----->
'-Format----+Standard+-'
                    '-Detailed-'

.-CODEType----BOTH-----.
```

```

>----->
'-CODEType---+UNICODE---+'
      +-NONUNICODE+
      '-BOTH-----'

.-NAMEType---SERVER-----
>----->
'-NAMEType---+SERVER---+' '-BEGINDate---fecha-'
      +-UNICODE+
      '-FSID----'

>----->
'-BEGINTime---hora-' '-ENDDate---fecha-'

.-ALLStats---No-----
>-----<
'-ENDTime---hora-' '-ALLStats---+Yes+-'
                    '-No--'

```

Parámetros

nombre_agrupación

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio cuyos datos se incluyen en las estadísticas de deduplicación de datos. Este parámetro es opcional. Si no especifica un valor para este parámetro, se visualizarán todas las agrupaciones de almacenamiento. Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el mandato falla.

Restricción: Sólo puede especificar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de nube.

nombre_nodo

Especifica el nombre del nodo de cliente cuyos datos se incluyen en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Si no especifica un valor para este parámetro, se visualizarán todos los nodos. Puede especificar hasta 64 caracteres para el nombre de nodo. Si especifica más de 64 caracteres, el mandato falla.

nombre_espacio_de_archivos o FSID

Especifica el nombre de uno o varios espacios de archivos que contienen los datos que se van a incluir en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se muestran todos los espacios de archivos. Puede especificar varios nombres separándolos con comas y sin espacios intercalados.

Para un servidor que tiene clientes con soporte para espacios de archivos que están en formato Unicode, puede especificar un nombre de espacio de archivos o un identificador de espacio de archivos (FSID). Si especifica un nombre de espacio de archivos, puede que el servidor tenga que convertir el nombre del espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode.

Restricciones: Se aplican las restricciones siguientes a los nombres de espacio de archivos y FSID:

- Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.
- No mezcle los FSID y los nombres de espacio de archivos en el mismo mandato.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. Especifique uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial sobre los conjuntos de eliminación de duplicados de datos especificados. Este es el valor predeterminado.

Detailed

Especifica que se visualizará información completa sobre los conjuntos de eliminación de duplicados de datos especificados.

CODEType

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Especifique uno de los siguientes valores:

UNICODE

Incluir los espacios de archivos que están en formato Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en formato Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos. Este es el valor predeterminado.

NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes con soporte para los espacios de archivos que están en formato Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que utilizan sistemas operativos Windows, NetWare o Macintosh OS X. Utilice este parámetro sólo cuando especifique un nombre de nodo y un nombre de espacio de archivos o un FSID. Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un comodín.

Especifique uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus FSID.

BEGINDate

Especifica la fecha de inicio para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora es a las 12:00 de la noche de la fecha que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	15/09/2015
TODAY	La fecha actual.	TODAY
TODAY -días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los registros que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora de inicio para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha es la fecha actual a la hora que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	10:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00.

ENDDate

Especifica la fecha de finalización para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha. Si

especifica una fecha de finalización sin una hora final, la hora es a las 11:59:59 de la noche de la fecha de finalización especificada.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY -días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los registros que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora de finalización del rango para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha. Si especifica una hora final sin una fecha final, la fecha es la fecha actual a la hora que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	10:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha de finalización especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha de finalización especificada	NOW-02:00 o -02:00.

ALLStats

Especifica si se deben mostrar todas las estadísticas de eliminación de duplicados de datos o sólo las estadísticas de eliminación de duplicados de datos generadas más recientemente. Este parámetro es opcional. Especifique uno de los siguientes valores:

No

Muestra sólo las estadísticas de eliminación de duplicados de datos que se han generado más recientemente para cada nodo y espacio de archivos.

Yes

Muestra todas las estadísticas de eliminación de duplicados de datos.

Ejemplo: ver estadísticas de eliminación de duplicados de datos en formato estándar

Vea las estadísticas de eliminación de duplicados de datos para una agrupación de almacenamiento denominada POOL1. Las estadísticas de eliminación de duplicados de datos son para el nodo NODE1 y se muestran las estadísticas del 8 de mayo de 2015. Consulte Descripciones de los campos para ver una descripción de los campos.

```
query dedupstats pool1 node1 begindate=05/08/2015
```

```

Date/Time: 05/05/2015 15:15:23
Nombre agrupación almacenamiento: POOL1
Nombre nodo: NODE1
Nombre espacio archivos: \\fs1\al
FSID: 41
Tipo: C.S.
Porcentaje total de ahorro: 86,62
Total de datos protegidos (MB): 311

```

Ejemplo: ver estadísticas de eliminación de duplicados de datos detalladas

Vea información detallada para la eliminación de duplicados de datos de una agrupación de almacenamiento denominada POOL1.

```
query dedupstats pool1 format=detailed

        Date/Time: 05/05/2015 15:15:23
Nombre agrupación almacenamiento: POOL1
        Nombre nodo: NODE1
        Nombre espacio archivos: \\fs1\al
            FSID: 41
            Tipo: C.S.
Total de datos protegidos (MB): 47.646
Espacio total utilizado (MB): 10.139
Espacio total ahorrado (MB): 37.507
Porcentaje total de ahorro: 78,72
Ahorro de deduplicación: 16.228.107.499
Porcentaje de deduplicación: 42,59
Recuento de extensiones sin duplicados eliminados: 1.658
Espacio de extensión no deduplicado utilizado: 732.626
    Recuento de extensiones exclusivas: 189.791
    Espacio de extensión exclusivo utilizado: 23.385.014.635
    Recuento de extensiones compartidas: 178.712
Datos de extensiones compartidas protegidos: 26.575.010.669
Espacio de extensiones compartidas utilizado: 5.267.815.421
Ahorro de compresión: 5.267.815.421
Porcentaje de compresión: 62,93
Recuento de extensiones comprimidas: 352.498
Recuento de extensiones no comprimidas: 17.663
Espacio de extensión cifrada utilizado: 52.901.672
    Encryption Percentage: 100.00
    Encrypted Extent Count: 188
    Unencrypted Extent Count: 0
```

Descripciones de los campos

Fecha/hora

Muestra la fecha y la hora en las que se han generado las estadísticas de eliminación de duplicados de datos.

Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

Nombre del nodo

El nombre del nodo de cliente cuyos datos se incluyen en las estadísticas de eliminación de duplicados de datos.

Nombre de espacio de archivos

El nombre del espacio de archivos.

FSID

El nombre del identificador del espacio de archivos.

Tipo

El tipo de datos. Son posibles los siguientes valores:

Arch

Datos que se han archivado.

C.S.

Datos de los que se ha realizado una copia de seguridad.

G.E.

Datos que se han migrado desde un cliente IBM Spectrum Protect for Space Management.

Total de datos protegidos (MB)

La cantidad lógica de datos, en megabytes, protegidos en la agrupación de almacenamiento antes de la deduplicación y la compresión de datos. Este valor representa la suma de los valores de Espacio total utilizado (MB) y Espacio total ahorrado (MB).

Espacio total utilizado (MB)

La cantidad total de espacio utilizado en la agrupación de almacenamiento, en megabytes. Este valor es la cantidad física de datos de los que realizan copias de seguridad tras la deduplicación de datos y la compresión.

Espacio total ahorrado (MB)

La cantidad total de espacio, en megabytes, de datos que se han eliminado de la agrupación de almacenamiento debido a la deduplicación de datos y la compresión. Este valor representa la suma de los valores de Ahorro de deduplicación y Ahorro de compresión.

Porcentaje total de ahorro

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la compresión y la deduplicación de datos.

Ahorro de deduplicación

La cantidad de espacio utilizado que se ha ahorrado en la agrupación de almacenamiento debido a la deduplicación de datos.

Porcentaje de eliminación de duplicados

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la deduplicación de datos.

Recuento de extensiones no deduplicadas

El número de extensiones de datos donde no se han eliminado los duplicados en la agrupación de almacenamiento.

Espacio de extensión no deduplicado utilizado

La cantidad de espacio utilizado por extensiones de datos que no se han deduplicado en la agrupación de almacenamiento. Este valor se aplica a los contenedores con un tipo de archivo .ncf que no tienen datos duplicados eliminados.

Consejo: Las extensiones de datos cuyos duplicados no se han eliminado constan de los siguientes tipos de archivos o datos:

- Metadatos de archivo.
- Archivos de menos de 2 KB.
- Archivos que utilizan el cifrado del cliente.

Recuento de extensiones exclusivas

El número de extensiones de datos que no están compartidas por un nodo.

Espacio de extensión exclusiva utilizado

La cantidad de espacio en la agrupación de almacenamiento que no comparte un nodo. Este valor se aplica a los contenedores con un tipo de archivo .dcf que no tienen datos duplicados eliminados.

Recuento de extensiones compartidas

El número de extensiones de datos que se utilizan varias veces en el mismo nodo o en nodos distintos debido a la deduplicación de datos.

Datos de extensiones compartidas protegidas

La cantidad de espacio de la agrupación de almacenamiento que está protegido por extensiones de datos compartidas antes de la deduplicación de datos.

Espacio de extensión compartida utilizado

La cantidad de espacio de la agrupación de almacenamiento que utilizan las extensiones de datos compartidas tras la deduplicación de datos.

Ahorro de compresión

Cantidad de espacio utilizado que se ha ahorrado en la agrupación de almacenamiento debido a la compresión tras la deduplicación de datos.

Porcentaje de compresión

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la compresión.

Recuento de extensiones comprimidas

El número de extensiones de datos que se han comprimido.

Recuento de extensiones descomprimidas

El número de extensiones de datos que se han descomprimido.

Espacio de extensión cifrada utilizado

La cantidad de espacio en la agrupación de almacenamiento utilizado por extensiones de datos cifradas.

Porcentaje de cifrado

Porcentaje de datos cifrados en la agrupación de almacenamiento.

Recuento de extensiones cifradas

El número de extensiones de datos que se han cifrado.

Recuento de extensiones sin cifrar

El número de extensiones de datos que no se han cifrado.

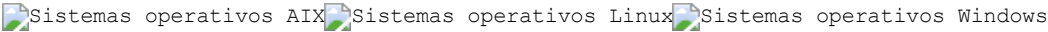
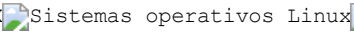
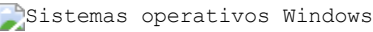

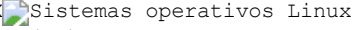
Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DEDUPSTATS

Mandato	Descripción
DELETE DEDUPSTATS	Suprime las estadísticas de eliminación de duplicados de datos.
GENERATE DEDUPSTATS	Genera las estadísticas de eliminación de duplicados de datos.

QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)

Utilice este mandato para visualizar información sobre una o varias clases de dispositivo.

Período de reintento:
 Intervalo entre reintentos:
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
 Compartido:
 Sistemas operativos AIX  Sistemas operativos Linux Asignación primaria (MB):
 Asignación secundaria (MB):
 Compresión:
 Retención:
 Protección:
 Fecha caducidad:
 Unidad:
 Protección de bloques lógicos:
 Última actualización por (administrador): ADMIN
 Fecha/hora última actualización: 05/31/2000 13:15:36

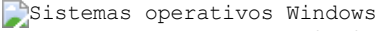
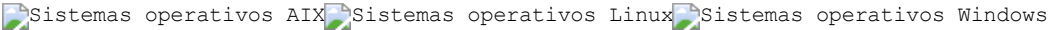
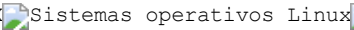
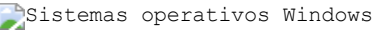

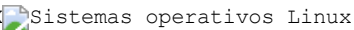
Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información detallada para una clase de dispositivo 3592 específica

Visualizar detalles completos sobre la clase de dispositivo 3592.

```
query devclass 3592 format=detailed
```

```

    Nombre clase dispositivo: 3592
    Estrategia acceso dispositivo: Secuencial
    Número agrupaciones almacenamiento: 1
    Tipo dispositivo: 3592
    Formato: 3592
    Capacidad est/máx (MB):
    Límite montaje: DRIVES
    Espera montaje (min): 60
    Espera montaje (min): 60
    Prefijo etiqueta: ADSM
 Sistemas operativos Windows Letra unidad:
    Biblioteca: MANLIB
    Directorio:
    Nombre servidor:
    Período de reintento:
    Intervalo entre reintentos:
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
    Compartido:
    Dirección de alto nivel:
    WORM: No
    Capacidad de escala: 90
    Cifrado de unidad: Activado
 Sistemas operativos AIX  Sistemas operativos Linux Asignación primaria (MB):
    Asignación secundaria (MB):
    Compresión:
    Retención:
    Protección:
    Fecha caducidad:
    Unidad:
    Protección de bloques lógicos: Lectura/Grabación
    Última actualización por (administrador): SERVER_CONSOLE
    Fecha/hora última actualización: 08/04/03 14:28:31
  
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre clase dispositivo

El nombre de la clase de dispositivo.

Estrategia acceso a dispositivo

Especifica cómo se graban los datos en la clase de dispositivo.

Número agrupaciones almacenamiento

El número de agrupaciones de almacenamiento asignadas a la clase de dispositivo.

Tipo dispositivo

El tipo de dispositivo de la clase de dispositivo.

Format

El formato de grabación.

Capacidad est/máx (MB)

La capacidad máxima o estimada de un volumen asociado con la clase de dispositivo.

Límite montajes

El número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente o especifica que DRIVES es el límite de montaje.

Espera montaje (min)


El número máximo de minutos que debe esperarse a que se monte un volumen de acceso secuencial.


Retención montaje (min)

El número de minutos que debe retenerse un volumen de acceso secuencial desocupado antes de desmontarlo.

Prefijo de etiquetas

El calificador de alto nivel del nombre del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial.

 Sistemas operativos Windows Letra unidad

 Sistemas operativos Windows La letra de unidad de un archivo extraíble.

Biblioteca

El nombre del objeto de biblioteca definido que contiene las unidades que utiliza la clase de dispositivo.

Directorio

Directorio o directorios de una clase de dispositivo FILE compartida.

Nombre servidor

El nombre de un servidor definido.

Período de reintento

El intervalo durante el cual el servidor intenta ponerse en contacto con un servidor de destino en caso de que se sospeche de que existe un problema de comunicaciones.

Intervalo entre reintentos

La frecuencia con la que se llevan a cabo los reintentos en un período de reintento.

Compartido

Si esta clase de dispositivo FILE se comparte entre el servidor y uno o más agentes de almacenamiento.

Dirección alto nivel

Dirección IP del dispositivo en formato decimal con puntos.

Capacidad mínima

La capacidad mínima de un volumen asociado con la clase de dispositivo.

WORM



Especifica si esta unidad es un dispositivo WORM (una sola grabación, varias lecturas).



Cifrado de unidad



Si se permite el cifrado de unidad. Este campo se aplica sólo a volúmenes de una agrupación de almacenamiento que está asociada a un tipo de dispositivo de 3592, LTO o ECARTRIDGE.



Capacidad de escala



Porcentaje de la capacidad del medio que puede utilizarse para almacenar datos.



 Sistemas operativos AIX  Sistemas operativos Linux Asignación principal (MB)



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo FILE que representan el almacenamiento que gestiona un servidor de medios de z/OS. Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen.



 Sistemas operativos AIX  Sistemas operativos Linux Asignación secundaria (MB)



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo FILE que representan el almacenamiento que gestiona un servidor de medios de z/OS. Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado.



 Sistemas operativos AIX  Sistemas operativos Linux Compresión



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica si los datos están comprimidos.



 Sistemas operativos AIX  Sistemas operativos Linux Retención

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica el número de días que se retiene la cinta, si se utiliza la retención.



 Sistemas operativos AIX  Sistemas operativos Linux Protección

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica si los volúmenes están protegidos por el programa RACF.

 Sistemas operativos AIX  Sistemas operativos Linux Fecha caducidad

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo, si se utiliza la caducidad.

 Sistemas operativos AIX  Sistemas operativos Linux Unidad

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica el nombre de unidad esotérico para el grupo de dispositivos de cinta.

Protección de bloques lógicos

Especifica si la protección de bloques lógicos está habilitada y, si lo está, la modalidad. Los valores posibles son Lectura/Grabación, Sólo lectura y No. Puede utilizar la protección de bloques lógicos solamente con los siguientes tipos de unidades y medios:

- IBM® LTO5 y posterior
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior
- Unidades Oracle StorageTek T10000C y T10000D

Última actualización por (administrador)









El administrador que ha realizado la última actualización de la clase de dispositivo.

Fecha/hora de la última actualización

Fecha y hora de la última actualización.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DEVCLASS

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
QUERY SERVER	Muestra información sobre servidores.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux UPDATE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Cambia los atributos de una clase de dispositivo para el almacenamiento gestionado por un servidor de medios de z/OS.

QUERY DIRSPACE (Consultar utilización de almacenamiento de directorios FILE)

Utilice este mandato para visualizar información acerca del espacio libre en los directorios relacionados con una clase de dispositivo con un tipo de dispositivo FILE.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query DIRSPace--+-+-----+-----><
                    '-nombre_clase_dispositivo-'
```

Parámetros

nombre_clase_dispositivo

Especifica el nombre de la clase de dispositivo que se ha de consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Se visualizarán todas las clases de dispositivos del tipo de dispositivo FILE coincidentes. Si no especifica un valor para este parámetro, se visualizarán todas las clases de dispositivos del tipo de dispositivo FILE.

Ejemplo: obtener una lista de las clases de dispositivo de tipo FILE

Visualizar información de todas las clases de dispositivo que tienen un tipo de dispositivo FILE. En el siguiente ejemplo, la unidad M equivale a megabytes y la unidad G equivale a gigabytes.

```
query dirspace
```

 Sistemas operativos Windows

Clase de dispositivo	Directorio	Capacidad estimada	Disponibilidad estimada
DBBKUP	/This/is/a/large/directory	13,000 M	5,543 M
DBBKUP	/This/is/directory2	13,000 M	7,123 M
DBBKUP2	/This/is/a/huge/directory	2,256 G	2,200 G

Sistemas operativos Windows

Clase de dispositivo	Directorio	Capacidad estimada	Disponibilidad estimada
DBBKUP	G:\This\is\a\large\directory	13,000 M	5,543 M
DBBKUP	G:\This\is\directory2	13,000 M	7,123 M
DBBKUP2	G:\This\is\a\huge\directory	2,256 G	2,200 G

Descripciones de los campos

Nombre clase dispositivo

El nombre de la clase de dispositivo.

Directorio

Vía de acceso del directorio ubicado en el servidor.

Capacidad estimada

Capacidad estimada total del directorio.

Disponibilidad estimada

Espacio disponible restante estimado para el directorio.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DIRSPACE

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.

QUERY DOMAIN (Consultar un dominio de políticas)

Utilice este mandato para visualizar información sobre uno o varios dominios de políticas.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-*-----
>>-Query Domain--+----->
      '-nombre_dominio-'

      .-Format----Standard----.
>--+-----><
      '-Format----+Standard-+-'
      '-Detailed-'

```

Parámetros

nombre_dominio

Especifica el dominio de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se visualizarán todos los dominios de políticas.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar un resumen de dominios de política

Visualizar información parcial de todos los dominios de políticas del servidor. Emita el mandato:

```
query domain
```

Nombre dominio políticas	Juego políticas activado	Clase gestión predeterm. activada	Número de nodos registrad.	Descripción
-----	-----	-----	-----	-----
EMPLOYEE- _RECORDS PROG1	VACATION	ACTIVEFI- LES	6	Dominio de registros de empleados
PROG2			0	Dominio de prueba de grupo de programación
STANDARD	STANDARD	STANDARD	1	Dominio de políticas instalado de forma dominio de políticas

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar la lista de agrupaciones de datos activos

Visualizar la lista de agrupaciones de datos activos. Emita el mandato:

```
query domain format=detailed
```

```
Nombre dominio políticas: STANDARD
Juego de políticas activado: STANDARD
Fecha/hora activación: 05/16/2006 16:18:05
Días desde activación: 15
Clase gestión predeterminada activada: STANDARD
Número de nodos registrados: 1
Descripción: Dominio de
políticas
predeterminado
instalado.

Retención copias seguridad (período gracia): 30
Retención copias archivadas (período gracia): 365
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 05/31/2006 15:17:48
Perfil de gestión:
Cambios pendientes: Si
Lista de agrupaciones de datos activos: ADPPPOOL
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de dominio de políticas

El nombre del dominio de políticas.

Juego de políticas activado

El nombre del último juego de políticas que se ha activado en el dominio.

Las definiciones del último juego de políticas activado y del el juego de políticas ACTIVE no son necesariamente idénticas. Al activar un juego de políticas, el servidor copia el contenido del juego de políticas en el juego de políticas con el nombre especial ACTIVE. Las definiciones copiadas que hay en el juego de políticas ACTIVE sólo se pueden modificar activando otro juego de políticas. Puede modificar el juego de políticas original sin que afecte al juego de políticas ACTIVE. Por lo tanto, las definiciones que hay en el último juego de políticas que se ha activado pueden ser distintas de las que hay en el juego de políticas ACTIVE.

Fecha/hora activación

La fecha y hora en que se ha activado el juego de políticas.

Días desde activación
El número de días transcurridos desde que se ha activado el juego de políticas.

Clase gestión predeterminada activada
La clase de gestión predeterminada asignada al juego de políticas.

Número de nodos inscritos
El número de nodos cliente registrados en el dominio de políticas.

Descripción
La descripción del dominio de políticas.

Retención copias seguridad (período gracia)
El número de días que se retienen las versiones de copia de seguridad inactivas de los archivos cuando existen algunas de las condiciones siguientes:

- Un archivo se vuelve a vincular a una nueva clase de gestión, pero ni la nueva clase de gestión ni la clase de gestión predeterminada contienen un grupo de copia de seguridad.
- La clase de gestión a la que está asociado un archivo no existe ya y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está asociado un archivo y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

Retención copias archivadas (período gracia)
El número de días que se retiene una copia archivada que cumple una de las condiciones siguientes:

- La clase de gestión a la que está asociado un archivo no existe ya y la clase de gestión predeterminada no contiene un grupo de copia de archivada.
- El grupo de copia de archivada se ha suprimido de la clase de gestión a la que está asociado un archivo y la clase de gestión predeterminada no contiene un grupo de copia archivada.

Última actualización por (administrador)
El administrador que ha definido o que ha actualizado más recientemente el dominio de políticas. Si este campo contiene \$\$CONFIG_MANAGER\$\$, el dominio de políticas está asociado a un perfil que gestiona el gestor de configuración.

Fecha/hora última actualización
Especifica cuándo ha definido o ha actualizado más recientemente el administrador el dominio de políticas.

Perfil de gestión
El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este dominio de políticas.

Cambios pendientes
Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

Lista de agrupaciones de datos activos
La lista de las agrupaciones de datos activos del dominio.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DOMAIN

Mandato	Descripción
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

QUERY DRIVE (Consultar información acerca de una unidad)

Utilice este mandato para visualizar la información sobre las unidades asociadas a una biblioteca.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

. - * * * ----- .

```

>>-Query DRive-----+-----+----->
      |                               .-*-----.|
      '-nombre_biblioteca-+-----+-'
                               '-nombre_unidad-'

.-Format-----Standard-----.
>-----+-----+-----+-----><
'-Format-----+Standard-+-'
      '-Detailed-'

```

Parámetros

library_name

Especifica el nombre de la biblioteca donde está situada la unidad consultada. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar este nombre.

Debe especificar un valor para este parámetro si especifica un nombre de unidad.

nombre_unidad

Especifica el nombre asignado a la unidad. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar este nombre. Si especifica un nombre de unidad, debe especificar también un valor para *nombre_biblioteca*.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial sobre la unidad.

Detailed

Especifica que se visualizará información completa sobre la unidad.

Ejemplo: obtener una lista de las unidades que se asocian al servidor

Visualizar información acerca de todas las unidades asociadas con el servidor. Emita el mandato:

```
query drive
```

Nombre bib.	Nombre unidad	Tipo dispos.	Activado
LIB1	DRIVE01	3590	Sí
LIB2	DRIVE02	3590	Sí

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información detallada acerca de una unidad y biblioteca específicas

Visualizar información detallada sobre la unidad denominada DRIVE02 asociada a la biblioteca LIB2. Emita el mandato:

```
query drive lib2 drive02 format=detailed
```

```

Nombre biblioteca: LIB2
Nombre unidad: DRIVE02
Tipo dispositivo: 3590
Activado: Yes
Estado de unidad: Empty
Asignado a:
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 29/02/2002 09:26:23
Frec. limpieza (Gigabytes/ASNEEDED/NONE): NONE

```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de biblioteca

Nombre de la biblioteca a la que se ha asignado la unidad.

Nombre de unidad

El nombre asignado a la unidad.

Tipo de dispositivo

El tipo de dispositivo especificado en la clase de dispositivo asociada. El servidor debe tener una ruta definida del servidor a la unidad para poder determinar el tipo de dispositivo verdadero. Siempre que haya una ruta definida del servidor a la unidad, el servidor mostrará el tipo de dispositivo verdadero de la unidad aunque haya otras rutas definidas en esta unidad. La excepción a esto se da cuando el tipo de dispositivo es remoto o desconocido.

REMOTE

El servidor no tiene una ruta al dispositivo. Las únicas rutas definidas al dispositivo proceden de los transportadores de datos.

UNKNOWN

No existe ninguna ruta.

Consejo: Revise la salida del mandato QUERY PATH para determinar si están definidas las rutas deseadas. Si no están definidas, defina las rutas deseadas mediante el mandato DEFINE PATH. Asimismo, si utiliza un dispositivo transportador de datos, revise la salida del mandato QUERY DATAMOVER para determinar el tipo del dispositivo transportador de datos. Si utiliza una ruta del servidor a una unidad, el tipo de dispositivo de la clase de dispositivo y la unidad deberán coincidir. Si utiliza una ruta de un dispositivo transportador de datos a una unidad, revise la documentación de su tipo de transportador de datos para asegurarse de que el tipo de dispositivo de la clase de dispositivo sea compatible con el tipo de dispositivo transportador de datos.

En línea

Especifica el estado de la unidad:

Sí

La unidad está activada y disponible para las operaciones de servidor.

No

La unidad está desactivada y un administrador la ha situado en este estado al actualizar el estado.

No disponible desde

Especifica que la unidad no está disponible desde *mm/dd/aa hh:mm:ss*. La salida muestra la hora en que el servidor marcó la unidad como no disponible.

Sondeando desde

Especifica que el servidor está sondeando la unidad ya que ésta ha dejado de responder. La salida muestra la hora en que el servidor detectó un problema y empezó a sondear. El servidor sondeará una unidad antes de indicar que no está disponible. La salida de la hora tiene el siguiente formato: *mm/dd/aa hh:mm:ss*.

Formatos de lectura

Los formatos de lectura de la unidad.

Formatos de grabación

Los formatos de grabación de la unidad.

Elemento

El número de elemento de la unidad.

Estado de la unidad

Especifica el estado actual de esta unidad basándose en el resultado del último mandato SCSI en la unidad o biblioteca. El servidor realiza el seguimiento del estado de la unidad para mejorar la selección de una unidad para una operación y para las operaciones de recuperación de la unidad. Los valores son:

Unavailable

La unidad no está disponible en la biblioteca para operaciones.

Empty

La unidad está vacía y lista para operaciones.

Loaded

La unidad está cargada actualmente y el servidor realiza operaciones en la unidad.

Unloaded

Se han expulsado los medios de la unidad.

Reserved

La unidad está reservada para una petición de montaje.

Desconocido

La unidad empieza en el estado de unidad desconocido como resultado de su definición, de la inicialización del servidor o porque se ha actualizado su estado a Activado.

Nombre de volumen

El nombre de volumen de la unidad.

Asignado a

El nombre del cliente de bibliotecas que actualmente utiliza la unidad. Esto sólo se aplica a las bibliotecas SCSI compartidas; el campo se deja en blanco para las demás bibliotecas.

WWN

El nombre de ámbito mundial de la unidad.

Última actualización por (administrador)

Especifica quién ha realizado la última actualización de la unidad.

Fecha/hora última actualización

Fecha y hora en las que tuvo lugar la última actualización.

Frec. limpieza (Gigabytes/ASNEEDED/NONE)

La frecuencia con que el servidor activa la limpieza de la unidad. Este valor puede ser el número de gigabytes, ASNEEDED o NONE.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DRIVE

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE DRIVE	Cambia los atributos de una unidad.

QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)

Utilice este mandato para visualizar información sobre volúmenes de copia de seguridad de base de datos y volúmenes en agrupaciones de almacenamiento, agrupaciones de almacenamiento de copia de contenedor y agrupaciones de almacenamiento de datos activos. También puede utilizar el mandato para crear un archivo de mandatos ejecutables para procesar los volúmenes.

El proceso de volúmenes por parte de este mandato depende del uso que se les de:

Copias de seguridad de la base de datos del servidor

Para controlar si el mandato procesa volúmenes de copia de seguridad de base de datos, utilice el parámetro SOURCE. El mandato puede procesar volúmenes utilizados para copias de seguridad de base de datos completas más las incrementales o de instantáneas. No se pueden especificar volúmenes virtuales (objetos de copia de seguridad almacenados en otro servidor). Puede modificar los volúmenes mediante cada estado, o bien utilizar el parámetro TOSTATE y omitir los estados para simplificar los traslados.

Agrupaciones de almacenamiento de copia

El mandato QUERY DRMEDIA siempre procesa volúmenes de agrupación de almacenamiento de copia que pueden seleccionarse.

Agrupaciones de almacenamiento de copia de contenedor

De forma predeterminada, los volúmenes de agrupación de almacenamiento de copia de contenedor no se pueden elegir para que las procese el mandato QUERY DRMEDIA. Para procesar volúmenes de agrupación de almacenamiento de copia de contenedor, debe emitir primero el mandato SET DRMCOPYCONTAINERSTGPOOL o especificar el parámetro COPYCONTAINERSTGPOOL en el mandato QUERY DRMEDIA.

Agrupaciones de almacenamiento de datos activos

De forma predeterminada, los volúmenes en agrupaciones de almacenamiento de datos activos no se pueden elegir para que las procese el mandato QUERY DRMEDIA. Para procesar volúmenes de agrupación de datos activos, debe emitir primero el mandato SET DRMACTIVEDATASTGPOOL o especificar el parámetro ACTIVEDATASTGPOOL en el mandato QUERY DRMEDIA.

Si utiliza una biblioteca externa y ha traspasado un volumen al estado NOTMOUNTBLE con el mandato MOVE DRMEDIA, puede que el mandato QUERY DRMEDIA todavía informe de que el estado del volumen es MOUNTABLE si detecta que el volumen se encuentra en la biblioteca. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que debería seguir al utilizar los mandatos MOVE DRMEDIA y QUERY DRMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Si el parámetro *CMD NO* está especificado: privilegio de operador o de sistema.
- Si el parámetro *CMD* está especificado y la opción del servidor *REQSYSAUTHOUTFILE* está establecida en *NO*: privilegio de operador, de almacenamiento sin restricciones o de sistema.

- Si el parámetro `CMD` está especificado y la opción del servidor `REQSYSAUTHOUTFILE` está establecida en `YES` (el valor predeterminado): privilegio de sistema.

Sintaxis

```

.*-----
>>-Query DRMedia-----+----->
      '-nombre_volumen-'

.-WHEREState---All-----
>-----+----->
  '-WHEREState---+-----+'
          +-All-----+
          +-MOUNTable-----+
          +-NOTMOUNTable----+
          +-COUrier-----+
          +-VAult-----+
          +-VAULTRetrieve---+
          +-COURIERRetrieve-+
          '-REmote-----'

>-----+-----+----->
  '-BEGINDate---fecha-' '-ENDDate---fecha-'

>-----+-----+----->
  '-BEGINTime---hora-' '-ENDTime---hora-'

>-----+-----+----->
  '-COPYstgpool---nombre_agrupación-'

>-----+-----+----->
  '-ACTIVEDatastgpool---nombre_agrupación-'

>-----+-----+----->
  '-COPYCONTainerstgpool---nombre_agrupación-'

.-Source---DBBackup----- .-Format---Standard-----
>-----+-----+----->
  '-Source---+DBBackup---+' '-Format---+Standard-+'
          +-DBSnapshot+           +-Detailed-+
          '-DBNone-----'         '-Cmd-----'

>-----+-----+----->
  '-WHERELOCation---ubicación-' | .----- |
                                |     V     |
                                '-Cmd---"mandato"-'

.-APPend---No-----
>-----+-----+-----<
  '-CMDfilename---nombre_archivo-' '-APPend---+No---+'
                                      '-Yes-'

```

Parámetros

nombre_volumen

Especifica los nombres de los volúmenes que se han de consultar. Puede utilizar caracteres comodín para especificar varios nombres. Este parámetro es opcional. El servidor busca nombres coincidentes de entre los siguientes volúmenes seleccionables:

- Volúmenes de copia de seguridad de base de datos, tal como estén seleccionados por el parámetro `SOURCE` de este mandato.
- Volúmenes de agrupación de almacenamiento de copia de agrupaciones de almacenamiento de copia especificados por el parámetro `COPYSTGPOOL`. Si no utiliza el parámetro `COPYSTGPOOL`, el servidor determinará qué volúmenes de las agrupaciones de almacenamiento de copia había especificado anteriormente el mandato `SET DRMCOPYSTGPOOL`.
- Los volúmenes de agrupación de almacenamiento de datos activos de las agrupaciones de almacenamiento de datos activos especificadas por parámetro `ACTIVEDATASTGPOOL`. Si no utiliza el parámetro `ACTIVEDATASTGPOOL`, el servidor consulta volúmenes de agrupaciones de almacenamiento de datos activos especificados anteriormente por el mandato `SET DRMACTIVEDATASTGPOOL`.
- Volúmenes de agrupación de almacenamiento de copia de contenedor de agrupaciones de almacenamiento de copia de contenedor especificadas por el parámetro `COPYCONTAINERSTGPOOL`. Si no utiliza el parámetro

COPYCONTAINERSTGPOOL, el servidor consulta volúmenes de agrupaciones de almacenamiento de copia de contenedor que fueron especificados previamente por el mandato SET DRMCOPYCONTAINERSTGPOOL.

El resto de parámetros también pueden limitar los resultados de la consulta.

WHEREState

Especifica el estado de los volúmenes que se han de procesar. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

All

Especifica todos los volúmenes con todos los estados.

MOuntable

Los volúmenes que se encuentran en este estado contienen datos válidos y son accesibles para el proceso en el local.

NOTMOuntable

Los volúmenes con este estado están en el local, contienen datos válidos y no son accesibles para procesos en el local.

COUrier

Los volúmenes con este estado se están trasladando a una ubicación fuera del local.

VAult

Los volúmenes con este estado están fuera del local, contienen datos válidos y no son accesibles para procesos en el local.

VAULTRetrieve

Los volúmenes con este estado se encuentran en la cámara de seguridad fuera del local y no contienen datos válidos.

- Se considera que un volumen de agrupación de almacenamiento de copia se encuentra en estado VAULTRETRIEVE si éste ha estado vacío durante, como mínimo, el número de días que se ha especificado con el parámetro REUSEDELAY del mandato DEFINE STGPOOL.
- Se considera que un volumen de copia de seguridad de base de datos se encuentra en estado VAULTRETRIEVE si éste se ha asociado a una serie de copias de seguridad de base de datos que ha caducado en función del valor que se ha especificado con el mandato SET DRMDBBACKUPEXPIREDDAYS.

Importante: Al emitir QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE, el servidor determina de forma dinámica qué volúmenes se pueden devolver al local para volver a utilizarlos o eliminarlos. Por tanto, para asegurarse de que identifica todos los volúmenes que se encuentran en estado VAULTRETRIEVE, emita QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE sin los parámetros BEGINDATE, ENDDATE, BEGINTIME ni ENDTIME. En el campo Fecha/hora última actualización de la salida de QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE se visualizan la fecha y la hora en las que un volumen se ha traspasado al estado VAULT, no al estado VAULTRETRIEVE.

COURIERRetrieve

Los volúmenes con este estado se devuelven a la ubicación en el local.

REmote

Los volúmenes con este estado contienen datos válidos y están ubicados en el servidor remoto fuera del local.

BEGINDate

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha más antigua en la que existe información del volumen. Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-7 o -7. Para consultar los volúmenes empezando por los registros cambiados al estado actual hace una semana, puede especificar BEGINDATE=TODAY-7 o BEGINDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM

Valor	Descripción	Ejemplo
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDDate

Especifica la fecha final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha actual.

Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-7 o -7. Para consultar los volúmenes empezando por los registros cambiados al estado actual hace una semana, puede especificar BEGINDATE=TODAY-7 o BEGINDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada con el parámetro BEGINDATE.

Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	12:33:28
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite el mandato QUERY DRMEDIA a las 09:00 con BEGINTIME=NOW+03:00 o con BEGINTIME=+03:00, El servidor visualiza los volúmenes que se han modificado al estado actual a las 12:00 en la fecha inicial especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30. Si emite el mandato QUERY DRMEDIA a las 09:00 con BEGINTIME=NOW-03:30 o con BEGINTIME=-03:30, El servidor visualiza los volúmenes que se han modificado al estado actual a las 5:30 en la fecha inicial especificada.

ENDTime

Especifica la hora final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con anterioridad respecto a la fecha y hora especificadas. El valor predeterminado son las 23:59:59.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite el mandato QUERY DRMEDIA a las 09:00 con ENDTIME=NOW+03:00 o con ENDTIME=+03:00, IBM Spectrum Protect procesará los volúmenes que han cambiado a su estado actual a las 12:00 de la fecha de finalización que ha especificado.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30 Si emite el mandato QUERY DRMEDIA a las 09:00 con ENDTIME=NOW-03:00 o con ENDTIME=-03:00, IBM Spectrum Protect procesará los volúmenes que han cambiado a su estado actual a las 06:00 de la fecha de finalización que ha especificado.

COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de copia que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento de copia especificadas con el mandato SET DRMCOPYSTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYSTGPOOL o si se han eliminado todas las agrupaciones de almacenamiento de copia con el mandato SET DRMCOPYSTGPOOL, el servidor procesará todos los volúmenes de agrupación de almacenamiento de copia que se encuentren en el estado especificado (ALL, MOUNTABLE, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE).

Source

Especifica si se selecciona algún volumen de copia de seguridad de base de datos. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Los valores posibles son:

DBBackup

Se seleccionan los volúmenes de copia de seguridad de base de datos completa e incremental.

DBSnapshot

Se seleccionan los volúmenes de copia de seguridad de instantánea de base de datos.

DBNone

No se selecciona ningún volumen de copia de seguridad de base de datos.

ACTIVEDatastgpool

Especifica el nombre de la agrupación de almacenamiento de datos activos cuyos volúmenes van a procesarse. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de datos activos que se han especificado con este parámetro alteran temporalmente las agrupaciones de almacenamiento de datos activos que se han especificado con el mandato SET DRMACTIVEDATASTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMACTIVEDATASTGPOOL se emitió anteriormente con nombres de agrupaciones de almacenamiento de datos activos válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMACTIVEDATASTGPOOL o todas las agrupaciones de almacenamiento de datos activos se han eliminado mediante el mandato SET DRMACTIVEDATASTGPOOL, el servidor procesa todos los volúmenes de agrupaciones de almacenamiento de datos activos cuyo estado sea el especificado (ALL, NOTMOUNTABLE, COURIER,

VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE). Los volúmenes que se encuentran en el estado MOUNTABLE no se procesarán.

COPYCONtainerstgpool

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de copia de contenedor especificadas usando este parámetro alteran temporalmente a aquellas especificadas usando el mandato SET DRMCOPYCONTAINERSTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYCONTAINERSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia de contenedor válidos, el servidor solo procesará dichas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYCONTAINERSTGPOOL, o si todas las agrupaciones de almacenamiento de copia de contenedor se han eliminado usando el mandato SET DRMCOPYCONTAINERSTGPOOL, el servidor procesará todos los volúmenes de agrupación de copia de contenedor basados en el valor especificado por el parámetro WHERESTATE. Si el parámetro está establecido en un valor ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE, los volúmenes se procesan. Si el valor está establecido en MOUNTABLE, los volúmenes no se procesan.

Format

Especifica la información que se visualizará. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará información detallada.

Cmd

Especifica que se han creado mandatos ejecutables para los volúmenes seleccionados. Si especifica FORMAT=CMD, también debe especificar el parámetro CMD.

WHERELOcation

Especifica la ubicación de los volúmenes que se han de consultar. Este parámetro es opcional. La longitud máxima de la lista de la ubicación es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Si especifica un nombre de servidor destino, el gestor de recuperación ante siniestro visualiza todos los volúmenes de copia de seguridad de base de datos y todos los volúmenes de agrupaciones de almacenamiento de copia ubicados en el servidor destino.

CMd

Especifica la creación de mandatos ejecutables para procesar el nombre de volumen y la ubicación que obtiene este mandato. Este parámetro es opcional. La especificación de mandatos ejecutables se ha de delimitar con comillas. La longitud máxima de este parámetro son 255 caracteres. El gestor de recuperación ante siniestro graba los mandatos en un archivo que se ha especificado mediante el parámetro CMDFILENAME o el mandato SET DRMCMDFILENAME o que ha generado el mandato QUERY DRMEDIA. Si la longitud del mandato es superior a 240 caracteres, se divide en varias líneas y se agregan caracteres de continuación (+). Tal vez necesite modificar el carácter de continuación según los requisitos del producto que ejecuta los mandatos.

Si no especifica el parámetro FORMAT=CMD, este mandato no creará líneas de mandatos.

serie

La serie de los mandatos. La serie no debe contener comillas intercaladas. Por ejemplo, éste es un parámetro CMD válido:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Éste es un ejemplo de un parámetro CMD *no* válido:

```
cmd=""checkin libvolume lib8mm" &vol status=scratch""
```

sustitución

Especifica una variable de sustitución para indicar a QUERY DRMEDIA que sustituya un valor por la variable. Las variables no son sensibles a las mayúsculas y minúsculas, y no deben contener espacios en blanco detrás del símbolo &. Las variables posibles son:

&VOL

Una variable de nombre de volumen.

&LOC



Una ubicación de volumen.



&VOLDSN

El nombre del archivo donde el servidor graba las etiquetas de los medios de acceso secuencial. Un ejemplo de un nombre de archivo de volumen de cinta de agrupación de almacenamiento de copia que utilice el prefijo TSM predeterminado es TSM.BFS. Un ejemplo de un nombre de archivo de volumen de cinta de copia de seguridad de base de datos que utilice el prefijo TSM310 definido con la clase de dispositivo es TSM310.DBB.

&NL

El carácter de nueva línea. Cuando se especifica &NL, el mandato QUERY DRMEDIA subdivide el mandato donde se encuentra la variable &NL y no añade un carácter de continuación. Debe especificar el carácter de continuación adecuado antes de &NL si es necesario. Si no se especifica &NL y la línea de mandatos es superior a 240 caracteres, la línea se divide en varias líneas y se agregan los caracteres de continuación (+).


 Sistemas operativos AIX  Sistemas operativos LinuxCMDFilename

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados con el parámetro CMD. Este parámetro es opcional.

Si no especifica un nombre con el mandato SET DRMCMDFILENAME, el servidor creará un nombre de archivo añadiendo `exec.cmds` al nombre de ruta absoluto del directorio de la instancia de IBM Spectrum Protect. Si especifica una serie nula (""), los mandatos sólo se visualizan en la consola. Puede redirigir los mandatos a un archivo mediante el carácter de redirección del sistema operativo.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

 Sistemas operativos WindowsCMDFilename

 Sistemas operativos WindowsEspecifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados con el parámetro CMD. Este parámetro es opcional.

Si no se especifica un nombre de archivo con el mandato SET DRMCMDFILENAME, el servidor crea un nombre de archivo añadiendo `exec.cmd` al directorio que representa esta instancia del servidor (normalmente el directorio en el que se instaló originalmente IBM Spectrum Protect). Si especifica una serie nula (""), los mandatos sólo se visualizan en la consola. Puede redirigir los mandatos a un archivo usando `> o >>`, que el sistema proporciona. El gestor de recuperación ante siniestro asigna el nombre de archivo especificado o generado. Si el archivo existe, el gestor de recuperación ante siniestro intenta utilizarlo, y se graba encima de los datos existentes.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

APPend

Especifica si se graba encima del contenido existente del archivo de mandatos o se agregan los mandatos al archivo. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

El gestor de recuperación ante siniestro sobregaba el contenido del archivo.

Yes

El gestor de recuperación ante siniestro añade los mandatos al archivo.

Ejemplo: obtener una lista de los volúmenes que se van a enviar al almacenamiento fuera del local

Visualizar todos los volúmenes que han de entregarse a un transportista para su almacenamiento fuera del local.

```
query drmedia wherestate=notmountable
format=standard
```

Nombre	Estado	Fecha/hora última actualización	Biblioteca automatizada
TAPE01	No montable	20/01/1998 14:25:22	
DBTP01	No montable	20/01/1998 14:25:22	
DBTP03	No montable	20/01/1998 14:31:53	

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información acerca de los volúmenes de la cámara de seguridad

Visualizar información detallada sobre todos los volúmenes que están en la cámara de seguridad.

```
query drmedia wherestate=vault format=detailed
```

```
Nombre volumen: DBTP02
Estado: Cámara seguridad
Fecha/hora última actualización: 20/01/1998 13:29:02
```

Ubicación: Ironmnt
 Tipo volumen: DBBackup
 Nombre agrupación almacenamiento copia:
 Nombre agrupación almacenamiento datos activos: TSMACTIVEPOOL
 Nombre biblioteca automatizada:

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de volumen

El nombre del volumen de copia de seguridad de base de datos o de agrupación de almacenamiento de copia.

Estado

El estado del volumen.

Fecha/hora última actualización

La fecha y la hora de la última actualización del estado del volumen. Para los volúmenes en estado de VAULTRETRIEVE, este campo muestra la fecha y la hora en las cuales se ha modificado un volumen al estado de VAULT, no VAULTRETRIEVE. El servidor no "actualiza" volúmenes a VAULTRETRIEVE. En el momento de emitirse el mandato QUERY DRMEDIA, el servidor determina dinámicamente si los datos de los volúmenes de agrupación de almacenamiento de copia y los volúmenes de copia de seguridad de base de datos ya no son válidos y si éstos pueden devolverse al local para su reutilización o desecho.

Ubicación

El campo Ubicación aparece cuando el volumen no puede montarse o no está la biblioteca. El campo Ubicación está vacío si el volumen puede montarse y está en la biblioteca.

Tipo volumen

El tipo del volumen. Los valores posibles son:

DBBackup

Volumen de copia de seguridad de base de datos completa o incremental.

DBSnapshot

Volumen de copia de seguridad de instantánea de base de datos.

CopyStgPool

Volumen de agrupación de almacenamiento de copia.

ContcopyStgPool

Un volumen de agrupación de almacenamiento de copia de contenedor.

Nombre agrupación almacenamiento copia

Para un volumen de agrupación de almacenamiento de copia, el nombre de la agrupación de almacenamiento de copia.

Nombre de la agrupación de almacenamiento de datos activos

Para un volumen de agrupación de almacenamiento de datos activos, el nombre de la agrupación de almacenamiento de datos activos.

Nombre agrupación almacenamiento copia contenedor

Para un volumen de agrupación de almacenamiento de copia de contenedor, el nombre de la agrupación de almacenamiento de copia de contenedor.




Biblioteca automatizada

El nombre de la biblioteca automatizada si el volumen está en una biblioteca.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DRMEDIA

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.

Mandato	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL	Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.
SET DRMFILEPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.

QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)

Utilice este mandato para visualizar la información sobre los parámetros del sistema que se han definido para el gestor de recuperación ante siniestro (DRM).

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query DRMStatus-----<<
```

Parámetros

Ninguno.

Ejemplo: visualizar información acerca de los parámetros del sistema de DRM

Visualizar información acerca de los parámetros del sistema de DRM:

```
query drmstatus

    Prefijo plan recuperación:
    Prefijo instrucciones plan:
    Sufijo volumen sustitución: @
    Agrupaciones almacenamiento primarias: PRIM1 PRIM2
    Agrupaciones almacenamiento de copia: COPY*
    Agrupaciones almacenamiento datos activos: TSMACTIVEPOOL
    Agrupaciones de almacenamiento de copia de contenedor: COPYCNTRPOOL
    Nombre ubicación no montable: Local
    Nombre transportista: Fedex
    Nombre ubicación cámara seguridad: Ironmnt
    Días caducidad serie copia seguridad BD: 30 Día(s)
    Días de caducidad del archivo del plan de recuperación: 30 día(s)
    ¿Comprobar etiqueta?: No
    ¿Procesar tipo dispositivo FILE?: No
    Nombre archivo mandatos:
```

Descripciones de los campos

Prefijo plan recuperación

Parte de prefijo especificada por el usuario del nombre del archivo del plan de recuperación.

Prefijo de instrucciones del plan

Parte de prefijo especificada por el usuario de los nombres de los archivos de instrucciones de recuperación del servidor.

Sufijo volumen sustitución

El carácter agregado al final de los nombres de volúmenes de sustitución del archivo del plan de recuperación.

Agrupaciones de almacenamiento primarias

Las agrupaciones de almacenamiento primarias que pueden seleccionarse para que las procese el mandato PREPARE. Si este campo está en blanco, se podrán seleccionar todas las agrupaciones de almacenamiento primarias.

Agrupaciones de almacenamiento de copia

Las agrupaciones de almacenamiento de copia que pueden seleccionarse para que las procesen los mandatos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, se podrán seleccionar todas las agrupaciones de almacenamiento de copia.

Agrupaciones de almacenamiento de datos activos

Las agrupaciones de datos activos que pueden seleccionarse para que las procesen los mandatos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, no se podrán seleccionar agrupaciones de datos activos.

Agrupaciones de almacenamiento de copia de contenedor

Las agrupaciones de almacenamiento de copia de contenedor que pueden seleccionarse para que las procesen los mandatos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, no se podrán seleccionar agrupaciones de almacenamiento de copia de contenedor.

Nombre ubicación no montable

El nombre de la ubicación fuera del local donde se almacenará el medio que se envía.

Nombre del transportista

El nombre del transportista que se utiliza para transportar el medio a la cámara de seguridad.

Nombre de ubicación de la cámara seguridad

El nombre de la cámara de seguridad donde se almacena el medio.

Días de caducidad de la serie de copia de seguridad de la base de datos

El número mínimo de días que deben transcurrir desde la creación de una serie de base de datos antes de que pueda darse caducidad a ésta. Consulte el mandato SET DRMDBBACKUPEXPIREDAYS para obtener información acerca de los criterios que deben satisfacerse para que tenga lugar la caducidad de una serie de copia de seguridad de base de datos.

Días de caducidad del archivo del plan de recuperación

El número mínimo de días que deben transcurrir desde la creación de un archivo de plan de recuperación, almacenado en un servidor de destino, antes de que pueda darse caducidad a éste. Consulte el mandato SET DRMRPFEXPIREDAYS para obtener información acerca de los criterios que deben satisfacerse para que tenga lugar la caducidad de un archivo de plan de recuperación.

¿Comprobar etiqueta?

Si han de leerse las etiquetas de medios de los volúmenes de medios secuenciales a los que se han dado de baja mediante el mandato MOVE DRMEDIA. Los valores posibles son Yes o No.

¿Procesar tipo dispositivo FILE?




Si los mandatos MOVE DRMEDIA o QUERY DRMEDIA han de procesar los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo que tiene un tipo de dispositivo FILE. Los valores posibles son Yes o No.

Nombre de archivo de mandatos

El nombre del archivo con la ruta completa que contiene los mandatos ejecutables que ha generado el mandato MOVE DRMEDIA o el mandato QUERY DRMEDIA.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY DRMSTATUS

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
SET DRMCHECKLABEL	Especifica si IBM Spectrum Protect debe leer las etiquetas de volúmenes durante el proceso del mandato MOVE DRMEDIA.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsSET DRMCOPYCONTAINERSTGPOOL	Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.

Mandato	Descripción
SET DRMCOURIERNAME	Especifica el nombre del transportista del medio de recuperación ante siniestro.
SET DRMDBBACKUPEXPIREDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMFILPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.
SET DRMINSTRPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta de las instrucciones del plan de recuperación.
SET DRMPPLANVPOSTFIX	Especifica los nombres de los volúmenes de sustitución del archivo del plan de recuperación.
SET DRMPPLANPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta del plan de recuperación.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.
SET DRMVaultNAME	Especifica el nombre de la cámara de seguridad donde está almacenado el medio DRM.
SET DRMNOTMOUNTABLENAME	Especifica el nombre de ubicación del medio DRM que se ha de enviar fuera del local.

QUERY ENABLED (Consultar eventos activados)

Utilice este mandato para visualizar una lista de eventos activados o una lista de eventos desactivados, la que sea más corta de las dos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query--ENabled--++-CONSOLE-----+----->
      +-ACTLOG-----+
      +-EVENTSERVER----+
      +-FILE-----+
      +-FILETEXT-----+
      |                |
      |                | (1) |
      +-NTEVENTLOG-----+
      |                |
      |                | (2) |
      +-SYSLOG-----+
      +-TIVOLI-----+
      '-USEREXIT-----'
```

```
>+-----<
  +-NODEname----nombre_nodo-----+
  '-SERVername----nombre_servidor-'
```

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

Parámetros

receptor

Especifica un tipo de receptor para los eventos activados. Este parámetro es necesario. Los valores válidos son:

ACTLOG

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor.

CONSOLE

Especifica la consola estándar del servidor como receptor.

EVENTSERVER


Especifica el servidor de eventos como receptor.


FILE


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

NODENAME

Especifica un nombre de nodo a consultar. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para los eventos activados para el servidor donde se ejecuta este mandato.

SERVername

Especifica el nombre de servidor que se va a consultar. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para los eventos activados para el servidor donde se ejecuta este mandato.

Ejemplo: consultar al servidor acerca de eventos de consola

Consultar al servidor los eventos de servidor que se han activado para la consola. Existen 10000 eventos de servidor posibles. Se muestra una lista de los eventos activados o de los eventos desactivados (la lista que sea más corta).

```
query enabled console
```

Se han activado 9998 eventos para el receptor CONSOLE. Los eventos siguientes para el receptor CONSOLE:

```
ANR8409, ANR8410
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY ENABLED

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

QUERY EVENT (Consultar eventos planificados y realizados)

Utilice este mandato para visualizar el estado de los eventos planificados. Los parámetros de fecha y hora le permiten limitar la consulta a los eventos que se planificaron para que ocurrieran en las fechas y horas especificadas. Puede minimizar el tiempo necesario para procesar esta consulta limitando la salida a los eventos cuyos tiempos de inicio planificados pertenezcan a un rango de fecha y hora.

La sintaxis del mandato es diferente para consultas que se aplican a operaciones planificadas de cliente y para mandatos planificados de administración.

Tabla 1. Mandatos relacionados con QUERY EVENT

Mandato	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
DELETE EVENT	Elimina los registros de eventos antes de una fecha y hora especificadas.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.
SET RANDOMIZE	Especifica la aleatorización de las horas de inicio de un margen de las planificaciones en modalidad por sondeo de cliente.

- QUERY EVENT (Visualizar planificaciones de cliente)
Utilice el mandato QUERY EVENT para visualizar los eventos planificados y que se han completado para los clientes seleccionados.
- QUERY EVENT (Visualizar planificaciones de eventos de administración)
Utilice el mandato QUERY EVENT para visualizar los eventos planificados y que se han completado para las planificaciones de mandatos de administración seleccionadas.

QUERY EVENT (Visualizar planificaciones de cliente)

Utilice el mandato QUERY EVENT para visualizar los eventos planificados y que se han completado para los clientes seleccionados.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query EVent--nombre_dominio--nombre_planificación----->
. -Type-----Client-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
      |                   .-,------. |
      |                   V             | |
      +-----+-----nombre_nodo+--+
. -BEGINdate-----fecha_actual-. . -BEGINTime-----00:00-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -BEGINdate-----fecha-----' ' -BEGINTime-----hora--'
. -ENDDate-----fecha_final-. . -ENDTime-----23:59-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -ENDDate-----fecha-----' ' -ENDTime-----hora--'
. -EXceptiononly-----No----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -EXceptiononly-----+No--+-'
      ' -Yes-'
. -Format-----Standard----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
' -Format-----+Standard+--'
      ' -Detailed-'
```

Parámetros

- nombre_dominio (Necesario)
Especifica el nombre del dominio de políticas al que pertenecen las planificaciones. Puede utilizar un carácter comodín para especificar este nombre.
- nombre_planificación (Obligatorio)

Especifica el nombre de la planificación para la que se visualizan eventos. Puede utilizar un carácter comodín para especificar este nombre.

Type=Client

Especifica que la consulta visualiza los eventos de las planificaciones de cliente. Este parámetro es opcional. El valor predeterminado es CLIENT.

Nodes

Especifica el nombre del nodo cliente que pertenece al dominio de políticas especificado para el que se visualizan eventos. Puede especificar varios nodos cliente separándolos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nodos. Si no especifica un nombre de cliente, se visualizarán los eventos de todos los clientes que coincidan con los parámetros nombre de dominio y nombre de planificación.

BEGINDate

Especifica la fecha inicial del rango horario de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es la fecha actual.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7. Para consultar los eventos que estaban planificados para iniciarse durante los últimos siete días, especifique BEGINDATE=TODAY-7 ENDDATE=TODAY o BEGINDATE=-7 ENDDATE=TODAY.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es 00:00.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW+03:00 o BEGINTIME=+03:00. IBM Spectrum Protect visualizará los eventos a las 12:00 en la fecha de inicio especificada.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00. Si emite este a las 9:00 para consultar los eventos que estaban planificados para iniciarse durante las últimas 4 horas, puede especificar BEGINTIME=NOW-04:00 ENDTIME=NOW o BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect visualizará los eventos a las 5:00 en la fecha de inicio especificada.

ENDDate

Especifica la fecha final del rango horario para los eventos que se han de visualizar. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. Para el parámetro BEGINDATE, se utiliza el valor predeterminado.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-8 o -8. Para consultar los eventos planificados para iniciarse durante una semana que terminaba ayer, puede especificar BEGINDATE=TODAY-8 ENDDATE=TODAY-1 o BEGINDATE=-8 ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. El valor predeterminado es 23:59.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW ENDTIME=NOW+03:00 o BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-04:00 o -04:00

EXceptiononly

Especifica el tipo de información que desea sobre los eventos planificados o completados. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que se visualizará información sobre eventos pasados y proyectados.

Yes

Especifica que se visualizan los eventos que no se han podido ejecutar según estaba planificado.

Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualiza información parcial acerca de los eventos.

Detailed

Especifica que se visualiza información completa acerca de los eventos.

Visualizar información parcial para los eventos no satisfactorios

Visualizar información parcial acerca de todos los eventos planificados para DOMAIN1 que no se han ejecutado correctamente. Limitar la búsqueda al cliente denominado JOE. Limitar los eventos visualizados a los eventos planificados entre el 11 de febrero de 2001 (02/11/2001) y el 12 de febrero de 2001 (02/12/2001).

```
query event domain1 * nodes=joe begindate=02/11/2001
enddate=02/12/2001 exceptionsonly=yes
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
02/11/1999 01:00:00	02/11/1999 01:13:55	BACK1	JOE	No ejecutado
02/12/1999 01:00:00		DAILYBKP	JOE	No hecho

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Visualizar información parcial para eventos planificados de un cliente

Visualizar información completa para todos los eventos planificados para procesarse. Utilizar la fecha de inicio como la correspondiente a 10 días antes de la fecha de hoy y la finalización incluye la fecha de hoy.

```
query event * * begindate=today-10 enddate=today
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
02/04/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/04/2013 14:00:00	02/04/2013 14:12:49	VDATAMVR1-IN1	VDATAMVR1-T1	Completado
02/04/2013 14:30:00	02/04/2013 14:33:10	VDATAMVR1-IN2	VDATAMVR1-T2	Completado
02/04/2013 15:00:00	02/04/2013 15:01:49	VDATAMVR1-IN3	VDATAMVR1-T3	Completado
02/04/2013 15:30:00	02/04/2013 15:42:00	VDATAMVR1-IN4	VDATAMVR1-T4	Completado
02/05/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/05/2013 14:00:00	02/05/2013 14:05:22	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/05/2013 14:30:00	02/05/2013 14:32:53	VDATAMVR1-F2	VDATAMVR1-F2	Error 12
02/05/2013 15:00:00	02/05/2013 15:00:38	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/05/2013 15:30:00	02/05/2013 15:36:41	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/06/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/06/2013 14:00:00	02/06/2013 14:06:42	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/06/2013 14:30:00	02/06/2013 14:35:41	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/06/2013 15:00:00	02/06/2013 15:08:56	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/06/2013 15:30:00	02/06/2013 15:40:49	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/07/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/07/2013 14:00:00	02/07/2013 14:03:43	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/07/2013 14:30:00	02/07/2013 14:35:10	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/07/2013 15:00:00	02/07/2013 15:09:12	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/07/2013 15:30:00	02/07/2013 15:40:21	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/08/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/08/2013 14:00:00	02/08/2013 14:10:17	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/08/2013 14:30:00	02/08/2013 14:39:16	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/08/2013 15:00:00	02/08/2013 15:08:17	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/08/2013 15:30:00	02/08/2013 15:41:16	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/09/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/09/2013 14:02:16		VDATAMVR1-F1	VDATAMVR1-F1	Error 12
02/09/2013 14:30:00	02/09/2013 14:44:26	VDATAMVR1-F2	VDATAMVR1-F2	Error 12
02/09/2013 15:00:00	02/09/2013 15:06:24	VDATAMVR1-F3	VDATAMVR1-F3	Error 12
02/09/2013 15:30:00	02/09/2013 15:32:18	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/11/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/11/2013 14:00:00	02/11/2013 14:01:05	VDATAMVR1-F1	VDATAMVR1-F1	Error 12
02/11/2013 14:30:00	02/11/2013 14:31:42	VDATAMVR1-F2	VDATAMVR1-F2	Error 12

02/11/2013 15:00:00	02/11/2013 15:06:17	V DATAMVR1-F3	V DATAMVR1-F3	Error 12
02/11/2013 15:30:00	02/11/2013 15:30:19	V DATAMVR1-F4	V DATAMVR1-F4	Completado
02/12/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/12/2013 14:00:00	02/12/2013 14:03:37	V DATAMVR1-F1	V DATAMVR1-F1	Completado
02/12/2013 14:30:00	02/12/2013 14:33:07	V DATAMVR1-F2	V DATAMVR1-F2	Completado
02/12/2013 15:00:00	02/12/2013 15:03:56	V DATAMVR1-F3	V DATAMVR1-F3	Completado
02/12/2013 15:30:00	02/12/2013 15:36:44	V DATAMVR1-F4	V DATAMVR1-F4	Completado
02/13/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/13/2013 14:00:00	02/13/2013 14:06:24	V DATAMVR1-F1	V DATAMVR1-F1	Completado
02/13/2013 14:30:00	02/13/2013 14:34:50	V DATAMVR1-F2	V DATAMVR1-F2	Completado
02/13/2013 15:00:00	02/13/2013 15:15:01	V DATAMVR1-F3	V DATAMVR1-F3	Completado
02/13/2013 15:30:00	02/13/2013 15:30:18	V DATAMVR1-F4	V DATAMVR1-F4	Completado
02/14/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Futuro
02/14/2013 14:00:00		V DATAMVR1-F1	V DATAMVR1-F1	Futuro
02/14/2013 14:30:00		V DATAMVR1-F2	V DATAMVR1-F2	Futuro
02/14/2013 15:00:00		V DATAMVR1-F3	V DATAMVR1-F3	Futuro

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Visualizar información detallada para eventos planificados de un cliente

Visualizar información detallada acerca de los eventos planificados para que los procese el cliente DOC entre las 10:00 y las 11:00 horas el 1 de noviembre de 2005 (11/01/2005). Observe que cuando el estado es Error, se visualiza el código de resultado.

```
query event domain1 * nodes=doc begindate=11/01/2005
begintime=10:00 endtime=11:00 enddate=11/01/2005
exceptionsonly=yes format=detailed
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
11/01/2005 10:01:01	11/01/2005 10:03:46	T1	DOC	Error 8
11/01/2005 10:16:01	11/01/2005 10:16:10	T1	DOC	Error 4
11/01/2005 10:31:01	11/01/2005 10:33:08	T1	DOC	Hecho
11/01/2005 10:46:01		T1	DOC	Inexist.
11/01/2005 10:57:49	11/01/2005 10:58:07	T0	DOC	Error 12

Descripciones de los campos

Nombre de dominio de políticas

Especifica el nombre del dominio de políticas al que está asignada la planificación.

Nombre de la planificación

Especifica el nombre de la planificación que ha iniciado este evento.

Nombre del nodo

Especifica el cliente que está planificado para realizar la operación.

Inicio planificado

Especifica la fecha y hora de inicio planificadas para el evento.

Inicio real

Especifica la fecha y hora en las que el cliente ha iniciado el proceso de la operación planificada. No se visualizará ninguna información si la operación planificada no se ha iniciado.

Hecho

Especifica la fecha y hora en que se ha completado el evento planificado.

Estado

Especifica el estado del evento en el momento de emitirse el mandato QUERY EVENT. Son posibles los siguientes valores:

Hecho

Especifica que el evento planificado se ha completado.

No válido

Especifica que el cliente informa de un error al ejecutar la operación planificada y los reintentos sucesivos han fallado.

Error; no se ha reiniciado

Especifica un estado intermedio, cuando se interrumpe una sesión de cliente a causa de un error de comunicaciones o de haber excedido el tiempo de espera en el servidor. Cuando el evento se completa, este estado se puede modificar a un estado final de "Completado" o "Error".

Futuro

Especifica que el inicio del margen de puesta en marcha de los eventos es en el futuro. Este estado también indica que todavía no se ha creado un registro para este evento.

En curso

Especifica que el evento planificado se está ejecutando y que aún no ha informado del estado de finalización al servidor.

Compruebe periódicamente el estado de finalización del evento planificado. Si el estado no se actualiza en un período de tiempo razonable, consulte los archivos dsmsched.log y dsmererror.log del cliente para determinar porqué el cliente no ha informado del resultado de este evento al servidor. Si la copia de seguridad planificada es anómala, vuelva a ejecutar el evento planificado o realice una copia de seguridad incremental manual para asegurar la copia de seguridad de los datos.

No hecho

Especifica que el margen de puesta en marcha planificado para este evento ha pasado y la planificación no ha comenzado.

Pendiente

Especifica que el mandato QUERY EVENT se ha emitido durante el margen de puesta en marcha del evento, pero que todavía no se ha iniciado el proceso de la operación planificada.

Reiniciado

Especifica que el cliente ha intentado procesar la operación planificada de nuevo.

Cortado

Especifica que las comunicaciones con el cliente se han cortado antes de que el evento pudiera realizarse.

Iniciado

Especifica que el evento ha empezado a procesarse.

Incierto

Especifica que el estado del evento no se puede determinar. El servidor especifica *Incierto* si el mandato QUERY EVENT no encuentra un registro de eventos. No se encontrará un registro de eventos si el registro se ha suprimido o si el servidor no estaba disponible durante el margen de puesta en marcha planificado (la planificación no se ha iniciado en ningún momento). Los registros con el estado *Incierto* no se almacenan en la base de datos. Si no desea que se visualicen estos registros, especifique EXCEPTIONSONLY=YES o suprima la planificación si ya no la necesita.

Atención: Cuando se procesa una operación planificada sin haberla reiniciado dentro de su duración especificada, el campo Estado muestra *Iniciado*. Si la operación continúa más allá de la duración especificada, no se crea ningún registro de eventos. Si se emite una consulta una vez transcurrida la duración especificada, se mostrará el estado *Error* aunque la operación se encuentre todavía en ejecución. Una vez completada la operación, se crea un registro de eventos y la consulta posterior muestra el resultado en el campo de estado.

Resultado

Especifica el código de retorno del cliente que indica si la planificación se ha procesado correctamente. Si el código de retorno es un valor distinto a cero, consulte el registro de actividades del servidor, el registro de errores del cliente y el registro de planificación.

Código de retorno	Explicación
0	Todas las operaciones se han completado correctamente.
4	La operación se ha completado correctamente, pero algunos archivos no se han procesado.
8	La operación se ha completado con al menos un mensaje de aviso.
12	La operación se ha completado con al menos un mensaje de error. El número de mensajes de error no incluye ninguna notificación acerca de archivos omitidos.
-99	La operación ha fallado debido a que la sesión entre el cliente y el servidor ha finalizado por un motivo desconocido. Se desconoce si el cliente puede volver a conectarse con el servidor para completar el suceso de planificación.

Si una planificación incluye el parámetro ACTION=COMMAND, y el mandato no es un mandato de IBM Spectrum Protect, este puede producir otros valores en el campo Resultado.

Motivo

Especifica el motivo del código de retorno.

QUERY EVENT (Visualizar planificaciones de eventos de administración)

Utilice el mandato QUERY EVENT para visualizar los eventos planificados y que se han completado para las planificaciones de mandatos de administración seleccionadas.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query EVent--nombre_planificación--Type----Administrative-->
```

```

.-BEGINDate----fecha_actual-. .-BEGINTime----00:00-.
>-----+-----+-----+-----+-----+----->
'-BEGINDate----fecha-----' '-BEGINTime----hora--'

.-ENDDate----fecha_inicial-. .-ENDTime----23:59-.
>-----+-----+-----+-----+-----+----->
'-ENDDate----fecha-----' '-ENDTime----hora--'

.-EXceptiononly----No-----
>-----+-----+-----+-----+-----+----->
'-EXceptiononly----+No--+-'
                               '-Yes-'

.-Format----Standard----
>-----+-----+-----+-----+-----+-----<<
'-Format----+Standard+-'
                               '-Detailed-'

```

Parámetros

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación para la que se visualizan eventos. Puede utilizar caracteres comodín para especificar nombres.

Type=Administrative (Necesario)

Especifica que la consulta visualiza los eventos de las planificaciones de mandato de administración.

BEGINDate

Especifica la fecha inicial del rango horario de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es la fecha actual.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7. Para consultar los eventos que estaban planificados para iniciarse durante los últimos siete días, especifique BEGINDATE=TODAY-7 ENDDATE=TODAY o BEGINDATE=-7 ENDDATE=TODAY.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es 00:00.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW

Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW+03:00 o BEGINTIME=+03:00. IBM Spectrum Protect visualizará los eventos a las 12:00 en la fecha de inicio especificada.
NOW-HH:MM o - HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00. Si emite este a las 9:00 para consultar los eventos que estaban planificados para iniciarse durante las últimas 4 horas, puede especificar BEGINTIME=NOW-04:00 ENDTIME=NOW o BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect visualizará los eventos a las 5:00 en la fecha de inicio especificada.

ENDDate

Especifica la fecha final del rango horario para los eventos que se han de visualizar. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. Para el parámetro BEGINDATE, se utiliza el valor predeterminado. Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-8 o -8. Para consultar los eventos planificados para iniciarse durante una semana que terminaba ayer, puede especificar BEGINDATE=TODAY-8 ENDDATE=TODAY-1 o BEGINDATE=-8 ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. El valor predeterminado es 23:59.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW

Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW ENDTIME=NOW+03:00 o BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM o - HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-04:00 o -04:00

EXceptiononly

Especifica el tipo de información que desea sobre los eventos planificados o completados. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que se visualizará información sobre eventos pasados y proyectados.

Yes

Especifica que se visualizan los eventos que no se han podido ejecutar según estaba planificado.

Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualiza información parcial acerca de los eventos.

Detailed

Especifica que se visualiza información completa acerca de los eventos.

Ejemplo: obtener una lista de los eventos de una planificación de administración específica

Visualizar información parcial para todos los eventos planificados para la planificación de administración denominada DOSADMIN. La consulta se limitará a los eventos planificados para el 30 de marzo de 1999 (03/30/1999). Emita el mandato:

```
query event dosadmin type=administrative
begindate=03/30/1999
enddate=03/30/1999
```

Inicio planificado	Inicio real	Nombre archivos	Estado del cliente
03/30/1999 00:00:00	03/30/1999 00:00:01	DOSADMIN	Hecho
03/30/1999 04:00:00	03/30/1999 04:00:01	DOSADMIN	Hecho
03/30/1999 12:00:00		DOSADMIN	Futuro
03/30/1999 16:00:00		DOSADMIN	Futuro

Descripciones de los campos

Inicio planificado

Especifica la fecha y hora de inicio planificadas para el evento.

Inicio real

Especifica la fecha y hora en las que el cliente ha iniciado el proceso de la operación planificada. No se visualizará información si no se ha comenzado la ejecución de la planificación.

Nombre de la planificación

Especifica el nombre de la planificación que ha iniciado este evento.

Estado

Para los mandatos de administración o scripts donde se especifique WAIT=YES, el estado de un evento planificado es STARTED hasta que la operación especificada mediante el mandato o el script finalice. El estado final del evento planificado depende del código de retorno de la operación. Sin embargo, si WAIT=YES y la planificación ejecuta un script donde se especifica PREVIEW=YES, el estado final es COMPLETED, a menos que el script contenga un error de sintaxis.

Para los mandatos de administración o scripts donde se especifique WAIT=NO, el estado de un evento planificado es COMPLETED si el mandato o el script se ha iniciado. El éxito de la planificación dependerá del éxito de la operación realizada con el mandato o con el script.

NODENAME

Especifica un nombre de nodo a consultar. Puede utilizar un carácter comodín para especificar un nombre. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para las reglas de eventos para el servidor donde se ejecuta este mandato.

SERVER

Especifica el nombre de servidor que se va a consultar. Puede utilizar un carácter comodín para especificar un nombre. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para las reglas de eventos para el servidor donde se ejecuta este mandato.

Ejemplo: visualizar el historial de los eventos de cliente para la consola del servidor

Visualizar la información histórica de eventos de clientes activados o desactivados para la consola del servidor y los receptores de anotaciones de actividades.

```
query eventrules console,actlog nodename=*
```

Fecha/hora	Reglas eventos cliente
29/05/97 13:39:58	ENABLE EVENTS CONSOLE ANE4001 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4962 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4963 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4965 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4966 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4967 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4968 NODENAMES=JEE
30/05/97 14:24:20	ENABLE EVENTS CONSOLE ANE4015 NODENAMES=RON
30/05/97 14:24:50	ENABLE EVENTS CONSOLE ANE4026 NODENAMES=DONNA
30/05/97 14:25:59	ENABLE EVENTS CONSOLE ANE4015 NODENAMES=DONNA

Ejemplo: visualizar el historial de los eventos de cliente para todos los receptores

Visualizar la información histórica de los eventos del servidor activados o desactivados para todos los receptores.

```
query eventrules
```

Fecha/hora	Reglas eventos servidor
22/05/97 14:35:13	ENABLE EVENTS CONSOLE ANR2578
30/05/97 14:29:31	ENABLE EVENTS CONSOLE ANR0272
30/05/97 14:31:46	ENABLE EVENTS USEREXIT ANR0130
30/05/97 14:31:54	ENABLE EVENTS USEREXIT ANR0131
30/05/97 14:50:28	ENABLE EVENTS USEREXIT ANR0266

Descripciones de los campos

Date/Time

Especifica la fecha y hora en que se ha habilitado o inhabilitado el evento.

Reglas de eventos de cliente

Especifica los eventos de cliente que se habilitaron o inhabilitaron para los receptores especificados.

Reglas de eventos de servidor

Especifica los eventos de servidor que se habilitaron o inhabilitaron para los receptores especificados.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY ENABLED

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.

QUERY EVENTSERVER (Consultar el servidor de eventos)

Utilice este mandato para visualizar el nombre del servidor de eventos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query EVENTSERVER----->>
```

Ejemplo: visualizar el nombre del servidor de eventos

Visualizar el nombre del servidor de eventos.

```
query eventserver
```

```
ANR1669I Está definido como el servidor de eventos.
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY EVENTSERVER

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DEFINE EVENTSERVER	Define un servidor como un servidor de eventos.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE EVENTSERVER	Suprime la referencia a un servidor de eventos.
DELETE SERVER	Suprime la definición de un servidor.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.

QUERY EXPORT (Consultar las operaciones de exportación activas o suspendidas)

Utilice este mandato para obtener una lista de todas las operaciones de exportación reiniciables. Una exportación reinicial es una operación de exportación de servidor a servidor cuyo valor de FILEDATA no es NONE. Solamente se muestran las operaciones de exportación de servidor a servidor que se pueden suspender.

No se visualiza ninguna operación EXPORT NODE o EXPORT SERVER con FILEDATA=NONE. Asimismo, el mandato QUERY EXPORT no muestra las operaciones de exportación en las que el dispositivo de destino sea un medio secuencial o un volumen virtual.

Clase de privilegio

Este mandato lo puede emitir un administrador.

Sintaxis

```
>>-Query EXPort--+'-----+>
                '---identificador_exportación---'

.-State---All-----
>+-----+>
  '-State---All---+'
      +-Running---+
      '-SUSPended-'

>+-----+>
  '-PROcEss---process_number-'
```



```
nametype=unicode
filedata=archive
durunits=indefinite
toserver=athens
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información acerca de una operación de exportación en ejecución

Visualizar información acerca de la operación de exportación actualmente en ejecución que tiene el número de proceso "7". Emita el mandato siguiente:

```
query export process=7
```

Identificador exportación	Hora inicio	Estado	ID de proceso	Mandato
MYEXPORTNODE	01/24/2007 10:30:03	Ejecución	7	Export NODE me,you,them filespace=c\$\n nametype=unicode filedata=all toserver=athens exportid=MYEXPORTNODE

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información detallada acerca de todas las operaciones de exportación suspendidas.

Mostrar una lista con la información sobre todas las operaciones de exportación suspendidas. Emita el mandato siguiente:

```
query export state=suspended format=detailed
```

```
Identificador de exportación : MyExportNode
Hora de inicio : 24/01/2007 10:30:03
Estado : Suspendido
ID de proceso : --
Mandato: Export NODE m* filespace=c$\n
        nametype=unicode\n
        filedata=all\n
        durunits=indefinite\n
        toserver=athens\n
Fase : Lista de archivos\n
        finalizada. Exportando\n
        archivos seleccionables\n
Tiempo total de ejecución : 3 días 0 horas 24 minutos
Tiempo de ejecución del proceso actual :
Número de reinicios de operación\n
        de exportación : 0
Fecha y hora del último reinicio : --
Fecha y hora de la última suspensión : 25/01/2007 08:30:11
Dominios de políticas exportados : 0
Juegos de políticas exportados : 0
Planificaciones exportadas : 0
Clases de gestión exportadas : 0
Grupos de copia exportados : 0
Administradores exportados : 1
Conjuntos de opciones exportados : 0
Definiciones de nodos exportadas : 3
Definiciones de espacios de archivos exportadas : 7
Copias archivadas exportadas : 50.000
Archivos de copia de seguridad exportados : 150.000
Archivos bajo gestión de espacio exportados : 0
Copias archivadas omitidas : 0
Archivos de copia de seguridad omitidos : 25
Archivos bajo gestión de espacio omitidos : 0
Número total de bytes transferidos (MB) : 7.000
Número total de archivos por transferir : 900.000
Archivos restantes : 700.000
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información acerca de las operaciones de exportación de servidor a servidor

Mostrar una lista con la información detallada sobre todas las operaciones de exportación de servidor a servidor en ejecución. Emita el mandato siguiente:

```
query export state=running format=detailed
```

```
Identificador de exportación : export_HOME_Dirs
Hora de inicio : 25/01/2007 09:30:03
Estado : Ejecutando
ID de proceso : 11
Mandato: Export NODE n2,n3,n4
        filesystem=/home nametype=
        server
        filedata=all
        toserver=athens
Fase : Identificando y exportando
      archivos seleccionables
Tiempo total de ejecución : 0 días 22 horas 0
                          minutos
Tiempo de ejecución del proceso actual : 01:30:00
Número de reinicios de operación de exportación: 4
Fecha y hora del último reinicio : 01/02/2007 11:00:03
Fecha y hora de la última suspensión : 31/01/2007 05:01:00
Dominios de políticas exportados : 0
Juegos de políticas exportados : 0
Planificaciones exportadas : 0
Clases de gestión exportadas : 0
Grupos de copia exportados : 0
Administradores exportados : 1
Conjuntos de opciones exportados : 0
Definiciones de nodos exportadas : 3
Definiciones de espacios de archivos exportadas : 7
Copias archivadas exportadas : 0
Archivos de copia de seguridad exportados : 1000
Archivos bajo gestión de espacio exportados : 0
Copias archivadas omitidas : 0
Archivos de copia de seguridad omitidos : 0
Archivos bajo gestión de espacio omitidos : 0
Número total de bytes transferidos (MB) : 50
Número total de archivos por transferir : 400.000
Archivos restantes : 399.000
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Identificador de exportación

Identificador exclusivo asignado a esta operación de exportación de servidor a servidor.

Hora inicio

Hora y fecha en que se inició esta operación de exportación.

Estado

Estado actual de esta operación de exportación. El valor puede ser uno de los siguientes:

Ejecutando -- no suspendible

La operación está activa y está transmitiendo definiciones al servidor de destino. El proceso no se puede suspender y, si falla en este estado, no podrá reiniciarlo.

Ejecutando

La operación está activa y está buscando archivos seleccionables o bien transmitiendo definiciones al servidor de destino.

En ejecución - suspensión en curso

La operación está en proceso de ser suspendida como resultado de un mandato SUSPEND EXPORT. La operación de exportación está completamente suspendida cuando se guardan todos los datos de la operación de exportación. Una operación de exportación en este estado no responde a los mandatos siguientes:

- CANCEL PROCESS
- CANCEL EXPORT
- RESTART EXPORT
- SUSPEND EXPORT

Suspendido

La operación ha dejado de ejecutarse debido a un error o a que se ha suspendido con el mandato SUSPEND EXPORT.

ID de proceso

El ID de proceso para la operación de exportación cuando el estado es "Inicializando" o "Ejecutando".

Mandato

Mandato completo que se ha emitido para iniciar esta exportación de servidor a servidor.

Fase

Paso actual que está llevando a cabo la operación. Las fases posibles se muestran en el orden en el que se realizan:

Creando definiciones en el servidor de destino

La operación está exportando definiciones. El proceso no se puede suspender. Si el proceso falla en esta fase, no se podrá reiniciar.

Identificando y exportando archivos seleccionables

La operación está creando una lista de archivos seleccionables para exportarlos. Algunos archivos también se puede transmitir al destino en esta fase. Un proceso que está en esta fase se puede suspender. Si el proceso falla en esta fase, se podrá reiniciar.

Lista de archivos finalizada. Exportando archivos seleccionables

La operación ha acabado de crear la lista de archivos seleccionables para la exportación y está transmitiendo los archivos al destino. Un proceso que está en esta fase se puede suspender. Si el proceso falla en esta fase, se podrá reiniciar.

Tiempo total de ejecución

Tiempo que ha tardado en ejecutarse esta operación de exportación de servidor a servidor. Por ejemplo, si esta operación se inició y luego se suspendió y se inició dos veces, este valor corresponde al tiempo de ejecución total de los tres procesos activos de la operación de exportación.

Tiempo de ejecución de proceso actual

Tiempo que ha tardado en ejecutarse el proceso activo de una operación de exportación de servidor a servidor. No se visualizará ningún valor para una operación suspendida, pues no existe ningún proceso activo.

Cuenta de reinicio de operación de exportación

Número de veces que la operación de exportación de servidor a servidor se ha reiniciado.

Fecha y hora del último reinicio

Fecha y hora de la última vez que esta operación de exportación de servidor a servidor se ha reiniciado.

Fecha y hora de la última suspensión

Fecha y hora de la última vez que esta operación de exportación de servidor a servidor se ha suspendido.

Dominios de políticas exportados

Número de definiciones de dominios de políticas que se han exportado correctamente al servidor de destino.

Juegos de políticas exportados

Número de definiciones de juegos de políticas que se han exportado correctamente al servidor de destino.

Planificaciones exportadas

Número de definiciones de planificaciones que se han exportado correctamente al servidor de destino.

Clases de gestión exportadas

Número de definiciones de clases de gestión que se han exportado correctamente al servidor de destino.

Grupos de copia exportados

Número de definiciones de grupos de copia que se han exportado correctamente al servidor de destino.

Administradores exportados

Número de definiciones de administradores que se han exportado correctamente al servidor de destino.

Conjuntos de opciones exportados

Número de definiciones de conjuntos de opciones que se han exportado correctamente al servidor de destino.

Definiciones de nodos exportadas

Número de definiciones de nodos que se han exportado correctamente al servidor de destino.

Definiciones de espacio de archivos exportadas

Número de definiciones de espacios de archivos que se han exportado correctamente al servidor de destino.

Copias archivadas exportadas

Número de copias archivadas que se han exportado correctamente al servidor de destino.

Archivos de copia de seguridad exportados

Número de archivos de copia de seguridad que se han exportado correctamente al servidor de destino.

Archivos bajo gestión de espacio exportados

Número de archivos bajo gestión de espacio que se han exportado correctamente al servidor de destino.

Copias archivadas omitidas

Número de copias archivadas que se podían seleccionar para la exportación pero que se han omitido.

Archivos de copia de seguridad omitidos

Número de archivos de copia de seguridad que se podían seleccionar para la exportación pero que se han omitido.

Archivos bajo gestión de espacio omitidos

Número de archivos bajo gestión de espacio que se podían seleccionar para la exportación pero que se han omitido.

Número total de bytes transferidos (MB)

Número total de bytes transmitidos hasta el momento al servidor de destino en esta operación de exportación.

Número total de archivos por transferir

Número total de archivos transmitidos hasta el momento al servidor de destino en esta operación de exportación.




Archivos restantes

Número total de archivos que quedan por transmitir al servidor de destino en esta operación de exportación.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY EXPORT

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL EXPORT	Suprime una operación de exportación suspendida.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

Utilice este mandato para visualizar información sobre las actualizaciones de las extensiones de datos en las agrupaciones de almacenamiento de contenedores de directorio y para determinar qué extensiones de datos se suprimen y cuáles son elegibles para supresión.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query EXTENTUPdates--nombre_agrupación-----><
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que se consulta. No puede utilizar caracteres comodín para especificar este nombre.

Ejemplo: visualizar información sobre las actualizaciones de las extensiones de datos

Visualice información sobre las actualizaciones de las extensiones de datos emitiendo el siguiente mandato:

```
query extentupdates
```

```
    Número de extensiones pendientes de actualización: 0
    Número de extensiones no referenciadas: 0
    Número de extensiones elegibles para su supresión: 0
    Retardo de reutilización de extensión (días): 1
```

Consulte Descripciones de los campos para ver una descripción de los campos.

Descripciones de los campos

Número de extensiones pendientes de actualización

Especifica el número de referencias de extensión de datos que están pendientes de actualización en la agrupación de almacenamiento de contenedores de directorio. Los datos que se almacenan en la agrupación de almacenamiento de contenedores de directorio aumentan el número de referencias y la supresión de datos disminuye el número de referencias.

Número de extensiones no referenciadas

Especifica el número de extensiones de datos a las que no se hace referencia en la agrupación de almacenamiento de contenedores de directorio. Puede suprimir las extensiones de datos si no se hace referencia a ellas de nuevo en el periodo de retardo de reutilización que se especifica en el mandato DEFINE STGPOOL.

Número de extensiones elegibles para su supresión

Especifica el número de extensiones de datos que pueden suprimirse de la agrupación de almacenamiento. Las extensiones de datos exceden el periodo de retardo de reutilización que se ha especificado en el mandato DEFINE STGPOOL.

Retardo de reutilización de extensión (días)

Especifica el periodo de retardo de reutilización, en días, de las extensiones de datos.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY EXTENTUPDATES

Mandato	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.

QUERY FILESPACE (Consultar uno o más espacios de archivos)

Utilice este mandato para visualizar información acerca de los espacios de archivos que pertenecen a un nodo cliente. La salida de este mandato incluye los resultados de la última copia de seguridad incremental o réplica.

Consejo: Si un nodo tiene más de un espacio de archivos, puede emitir un mandato DELETE FILESPACE para uno de los espacios de archivos. No obstante, si emite un mandato QUERY FILESPACE para el nodo durante el proceso de supresión, la salida no muestra ningún espacio de archivos. Para obtener información precisa sobre los restantes espacios de archivos, emita el mandato QUERY FILESPACE cuando finalice el proceso de supresión.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query Filespace----->
. *- *-----
>+-----+-----+-----+-----+----->
|      . *----- |
| '-nombre_nodo-+' |
|      '-nombre_espacio_archivos-' |
|
|.-Format----Standard----.  .-NAMEType----SERVER-----|
>+-----+-----+-----+-----+-----+-----+----->
| '-Format----+Standard-+' | '-NAMEType----+SERVER-+-' |
|      '-Detailed-' |      '+UNICODE-+' |
|                        |      '-FSID----' |
|
|.-CODEType----BOTH-----|
>+-----+-----+-----+-----+-----><
| '-CODEType----+UNICODE-+-' |
|      '+NONUNICODE-+' |
|      '-BOTH-----' |
```

Parámetros

nombre_nodo

Especifica el nodo cliente al que pertenece el espacio de archivos. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado es especificar todos los nombres de nodo.

Debe especificar un valor para este parámetro si especifica un nombre de archivo.

nombre_espacio_archivos

Especifica el nombre del espacio de archivos que se ha de consultar. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. Si no especifica ningún valor, se consultan todos los espacios de archivos.

Si un servidor incluye clientes que utilizan espacios de archivos habilitados para Unicode, es posible que el servidor tenga que convertir el nombre que especifique. Por ejemplo, puede que el servidor deba convertir el nombre del espacio de archivos que especifique de la página de códigos del servidor a Unicode. Si desea obtener más información, consulte el parámetro NAMETYPE. Si no especifica ningún nombre de espacio de archivos o especifica sólo un único carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Puede utilizar el mandato QUERY FILESPACE para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos en el que desea realizar una consulta.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Puede especificar uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial sobre el espacio de archivos especificado.

Detailed

Especifica que se visualizará información completa sobre el espacio de archivos especificado.

NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y tienen sistemas operativos de Windows, Macintosh OS X y NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente cualificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

CODETYPE

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

UNICODE

Incluir sólo los espacios de archivos que están en Unicode.

NONUNICODE

Incluir sólo los espacios de archivos que no están en Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

Ejemplo: obtener una lista de todos los espacios de archivos

Consultar todos los espacios de archivos que están asociados con todos los nodos cliente.

```
query filespace
```

Nombre	Nombre esp.	FSID	Plataforma	Tipo esp.	¿Es el	Capacidad %	
Nombre	Nombre			Tipo	Espacio de archivos	Unicode?	Util
-----	-----	----	-----	-----	-----	-----	----
JOE	\\joe\c\$	1	WinNT	NTFS	Si	2.502,3	75,2
JOE	\\joe\d\$	2	WinNT	NTFS	Si	6.173,4	59,6

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: visualizar información de espacio de archivos detallada acerca de un espacio de archivos virtual

Visualizar información detallada para el espacio de archivos /HomeDir, que es una correlación de espacio de archivos virtual y que pertenece al nodo NAS NAS1.

```
query fileSPACE nas1 /HomeDir
```

Nombre	Nombre esp.	FSID	Plataforma	Tipo esp.	¿Es el	Capacidad %	
Nombre	Nombre			Tipo	Espacio de archivos	Unicode?	Util
NAS1	/HomeDir	1	NetApp	WAFL (VFS)	No	2.502,3	75,2

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Importante: Es posible que no vea los resultados esperados después de solicitar un formato detallado porque la aplicación de la API debe completar varios campos. Estos campos incluyen:

- Tipo de espacio de archivos
- Plataforma
- Capacidad
- Pct. util
- Fecha/hora inicio última copia seguridad
- Fecha/hora finalización última copia de seguridad

Para obtener más información sobre los campos específicos actualizados por la API, consulte la publicación *IBM Spectrum Protect: Utilización de la interfaz de programación de aplicaciones*.

Ejemplo: visualizar información de espacio de archivos detallada acerca de un espacio de archivos y nodo específicos

Visualizar información detallada acerca del espacio de archivos \\joe\c\$ que pertenece al nodo cliente JOE.

```
query fileSPACE joe \\joe\c$ nametype=unicode format=detailed
```

```
Nombre nodo: JOE
Nombre espacio archivos: \\joe\c$
Nombre esp. archivos hexadecimal: 5c5c6a6f655c6324
FSID: 1
Nombre del grupo de proximidad: FSGRP1
Plataforma: WinNT
Tipo espacio archivos: NTFS
¿Es el esp. de archivos Unicode?: Sí
Capacidad: 2.502,3
Pct. Util: 75,2
Fecha/hora inicio última copia seguridad:
Días desde inicio última copia de seguridad:
Fecha/hora finalización última copia seguridad:
Días desde finalización última copia seguridad:
Fecha/hora inicio última réplica: 12/02/2012, 12:42:00
Días desde inicio última réplica de nodo: 30
Fecha/hora finalización última réplica: 12/02/2012, 12:42:00
Días desde finalización última réplica: 30
Fecha/hora última copia de seguridad de cliente (UTC): 02/06/2013, 09:10:00
Fecha/hora último archivado de cliente (UTC): 02/06/2013, 09:10:00
Nombre de regla de réplica de copia de seguridad: ACTIVE_DATA
Estado de regla de réplica de copia de seguridad: ENABLED
Nombre de la regla de réplica de archivado: DEFAULT
Estado de regla de réplica de archivado: ENABLED
Nombre de regla de réplica de gestión de espacio: NONE
Estado de regla de réplica de gestión de espacio: DISABLED
En Tipo de riesgo: intervalo personalizado
Intervalo de riesgo : 2,222
Fuera de servicio: No
Fecha de fuera de servicio:
Dirección MAC:
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Importante: Es posible que no vea los resultados esperados después de solicitar un formato detallado porque la aplicación de la API tiene que completar varios campos. Estos campos incluyen:

- Tipo espacio archivos
- Plataforma
- Capacidad
- Pct. util
- Fecha/hora inicio última copia seguridad
- Fecha/hora finalización última copia de seguridad

Para obtener más información sobre los campos específicos actualizados por la API, consulte la publicación *IBM Spectrum Protect: Utilización de la interfaz de programación de aplicaciones*.

Nombre del nodo

Especifica el nombre del nodo cliente.

Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre espacio archivos hexadecimal

Especifica el nombre hexadecimal del espacio de archivos para el nodo cliente en formato UTF-8.

FSID

Especifica el identificador del espacio de archivos.

Nombre de grupo de proximidad

Nombre del grupo de proximidad, si lo hay, al que pertenece el espacio de archivos.

Plataforma

Especifica la plataforma del nodo cliente.

Tipo espacio archivos

Especifica el tipo del espacio de archivos.

El tipo de espacio de archivos con la agregación "(VFS)" denota que se trata de una asignación de espacio de archivos virtual para una ruta de directorio de un dispositivo NAS.

Espacio de archivos Unicode

Indica si el espacio de archivos es Unicode.

Capacidad

Especifica la cantidad de espacio, en megabytes, asignado a este espacio de archivos en el nodo cliente.

Para un espacio de archivos virtual que es una asignación de espacio de archivos virtual para una ruta de directorio, este campo representa la capacidad del espacio de archivos en el que se encuentra la ruta de directorio.

Pct. util

Especifica el porcentaje del espacio de archivos que está ocupado.

Para un espacio de archivos virtual que es una asignación de espacio de archivos virtual para una ruta de directorio, el porcentaje utilizado se calcula como el porcentaje de la capacidad del espacio de archivos que ocupaba el directorio en el momento de la última copia de seguridad completa.

Fecha/hora inicio última copia seguridad

Especifica la fecha y hora de inicio de la última copia de seguridad incremental del espacio de archivos.

Días desde inicio última copia seguridad

Especifica el número de días desde el inicio de la última copia de seguridad incremental del espacio de archivos.

Fecha/hora finalización última copia de seguridad

Especifica la fecha y hora de terminación de la última copia de seguridad incremental del espacio de archivos.

Días desde finalización última copia seguridad

Especifica el número de días desde que se terminó la última copia de seguridad incremental del espacio de archivos.

Fecha/hora inicio última réplica

Especifica la fecha y la hora en que se ha iniciado la última réplica de espacio de archivos.

Días desde inicio última réplica

Especifica el número de días desde que se ha iniciado la última réplica de espacio de archivos

Fecha/hora finalización última réplica

Especifica la fecha y la hora en que ha finalizado la última réplica de espacio de archivos.

Días desde finalización última réplica

Especifica el número de días desde que ha finalizado la última réplica de espacio de archivos

Fecha/hora última copia de seguridad de cliente (UTC)

La fecha y la hora, en hora UTC (Hora universal coordinada), de la última operación de copia de seguridad de este espacio de archivos.

Fecha/hora último archivado de cliente (UTC)

La fecha y la hora, en hora UTC (Hora universal coordinada), de la última operación de archivado de este espacio de archivos.

Nombre de norma de réplica de copia de seguridad

Especifica la regla de réplica que se aplica a los datos de copia de seguridad en el espacio de archivos. Son posibles los siguientes valores:

ALL_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL_DATA_HIGH_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE_DATA excepto que los datos se replican con una prioridad alta.

DEFAULT

Replica los datos de seguridad según la regla del cliente de nodo para los datos de seguridad. Si la regla del cliente para los datos de seguridad es DEFAULT, los datos de seguridad se replican según la regla del servidor para los datos de seguridad.

NONE

Los datos de copia de seguridad en el espacio de archivos no se replican.

Estado de norma de réplica de copia de seguridad

Especifica si la réplica de los datos de copia de seguridad en el espacio de archivos está activada o desactivada. Si el estado es ENABLED, los archivos de copia de seguridad pueden replicarse. Si el estado es DISABLED, los archivos de copia de seguridad no pueden replicarse.

Nombre de norma de réplica archivada

Especifica la regla de réplica que se aplica a los datos de archivado en el espacio de archivos. Son posibles los siguientes valores:

ALL_DATA

Replica los datos de archivado. Los datos se replican con una prioridad normal.

ALL_DATA_HIGH_PRIORITY

Replica los datos de archivado. Los datos se replican con una prioridad alta.

DEFAULT

Replica los datos de archivado según la regla del cliente para los datos de archivado. Si la regla del cliente para los datos de archivado es DEFAULT, los datos de archivado se replican según la regla del servidor para los datos de archivado.

NONE

Los datos de archivado en el espacio de archivos no se replican.

Estado de norma de réplica archivada

Especifica si la réplica de los datos de archivado en el espacio de archivos está activada o desactivada. Si el estado es ENABLED, los archivos de archivado pueden replicarse. Si el estado es DISABLED, los archivos de archivado no pueden replicarse.

Nombre de norma de réplica de gestión de espacio

Especifica la regla de réplica que se aplica a los datos gestionados por espacio en el espacio de archivos. Son posibles los siguientes valores:

ALL_DATA

Replica los datos gestionados por espacio. Los datos se replican con una prioridad normal.

ALL_DATA_HIGH_PRIORITY

Replica los datos gestionados por espacio. Los datos se replican con una prioridad alta.

DEFAULT

Replica los datos gestionados por espacio según la regla del cliente para los datos gestionados por espacio. Si la regla del cliente para los datos gestionados por espacio es DEFAULT, los datos gestionados por espacio se replican según la regla del servidor para los datos gestionados por espacio.

NONE

Los datos gestionados por espacio en el espacio de archivos no se replican.

Estado de norma de réplica de gestión de espacio

Especifica si la réplica de los datos gestionados por espacio en el espacio de archivos está activada o desactivada. Si el estado es ENABLED, los archivos gestionados por espacio pueden replicarse. Si el estado es DISABLED, los archivos gestionados por espacio no pueden replicarse.

Tipo de riesgo

Especifica el tipo de evaluación de riesgo. Los valores pueden ser Predeterminado, Eludido o Personalizado. Predeterminado especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el mandato SET STATUSATRISKINTERVAL. Eludido especifica que el nodo no se evalúa para el estado de riesgo por el supervisor de estado. Personalizado indica que el nodo se evalúa con el intervalo que se ha especificado mediante el mandato SET VMATRISKINTERVAL, en lugar del intervalo que se ha especificado mediante el mandato SET STATUSATRISKINTERVAL.

Intervalo de riesgo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en peligro. Este campo se aplica sólo cuando el tipo de riesgo es Personalizado.

Fuera de servicio

Especifica si la máquina virtual que representa el espacio de archivos está fuera de servicio.

Fecha de fuera de servicio

Especifica la fecha en la que la máquina virtual que representa el espacio de archivos ha quedado fuera de servicio.

Dirección MAC

Especifica la dirección de control de acceso a soportes (MAC) de los espacios de archivos de los que se ha hecho copia de seguridad para las máquinas virtuales VMWare. En el caso de que la máquina virtual tenga varias direcciones MAC, esta es la dirección con el valor más bajo.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY FILESPACE

Mandato	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
RENAME FILESPACE	Redenomina un espacio de archivos de cliente en el servidor.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

QUERY LIBRARY (Consultar una biblioteca)

Utilice este mandato para visualizar la información sobre las bibliotecas.

Número de serie:
Etiquetado automático: OVERWRITE
Volver a etiquetar para reutilizar: Sí
Última actualización por (administrador): DOCTOR_MIKE
Fecha/hora última actualización: 2002-12-05 15:24:53

Sistemas operativos Windows

Nombre biblioteca: EZLIFE
Tipo biblioteca: SCSI
ID ACS:
Categoría privada:
Categoría reutilizable:
Categoría reutilizable WORM:
Gestor externo:
Compartido: Sí
Fuera de LAN:
Obedecer retención de montaje:
Gestor de bibliotecas primario: EZSERVER
WWN:
Número de serie:
Etiquetado automático: OVERWRITE
Restaurar unidades: No
Volver a etiquetar para reutilizar: Sí
Última actualización por (administrador): DOCTOR_MIKE
Fecha/hora última actualización: 2000-12-05 15:24:53

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Nombre de biblioteca

El nombre de la biblioteca.

Tipo de biblioteca

El tipo de la biblioteca.

Identificador ACS

Especifica que la biblioteca es una biblioteca StorageTek controlada mediante StorageTek ACCLS (Automated Cartridge System Library Software).

Categoría privada

El número de categoría para los volúmenes privados que deben montarse por nombre.

La información que aparezca visualizada en este campo únicamente se aplica a un IBM® Tape Library Dataserver, modelo 3494 ó 3495.

Categoría reutilizable

El número de categoría que se utilizará para los volúmenes reutilizables de la biblioteca.

La información que aparezca visualizada en este campo únicamente se aplica a un IBM Tape Library Dataserver, modelo 3494 ó 3495.

Categoría reutilizable WORM

Indica el número de categoría utilizado por los volúmenes reutilizables WORM en la biblioteca.

La información que aparezca visualizada en este campo únicamente se aplica a un IBM Tape Library Dataserver, modelo 3494 ó 3495.

Gestor externo

La ubicación del gestor de bibliotecas externo donde el servidor puede enviar peticiones de acceso a medios.

Compartido

Especifica si esta biblioteca se comparte con otros servidores de IBM Spectrum Protect en la red de área de almacenamiento (SAN).

Fuera de LAN

Especifica si se utiliza una biblioteca externa para operaciones fuera de LAN.

Obedecer retención de montaje

Especifica si el servidor utiliza el valor definido para la retención de montaje en la clase de dispositivo asociada a esta biblioteca externa.

Gestor de bibliotecas primario

El nombre del servidor responsable del control del acceso a los recursos de biblioteca.

WWN



Nombre de ámbito universal del canal de fibra de la biblioteca.



Número de serie

Especifica el número de serie de la biblioteca que se está consultando.

Etiquetado automático

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas.

 Sistemas operativos AIX  Sistemas operativos Windows Restaurar unidades

 Sistemas operativos AIX  Sistemas operativos Windows Especifica si el servidor realiza un restablecimiento del destino cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

Volver a etiquetar para reutilizar

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables.

Última actualización por (administrador)

Especifica quién ha realizado la última actualización de la biblioteca.

Fecha/hora última actualización

Fecha y hora en las que tuvo lugar la última actualización.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY LIBRARY

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE LIBRARY	Suprime una biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

QUERY LIBVOLUME (Consultar un volumen de biblioteca)

Utilice este mandato para visualizar información acerca de uno o varios volúmenes que se han dado de alta en una biblioteca automatizada para que los utilice el servidor de IBM Spectrum Protect.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
..*----- .-*-----
>>-Query LIBVolume--+-----+----->
      '-nombre_biblioteca-' '-nombre_volumen-'

.-Format----Standard----.
>--+-----+----->>
      '-Format----+Standard+-'
      '-Detailed-'
```

Parámetros

library_name

Especifica el nombre de la biblioteca. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todas las bibliotecas.

nombre_volumen

Especifica el nombre del volumen. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todos los volúmenes.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

- Especifica que se visualizará información parcial.
- Detailed
- Especifica que se visualizará toda la información.

Ejemplo: obtener una lista de los volúmenes dados de alta para una biblioteca específica

Visualizar información acerca de todos los volúmenes que se dan de alta en la biblioteca denominada TAPE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query libvolume tape
```

Nombre bibl.	Nombre vol.	Estado	Propiet.	Últ. util.	Elemento inicio	Tipo disposit.
TAPE	000114	Reutilizable			1.000	LTO
TAPE	NY1602	Reutilizable			1.001	DLT

Ejemplo: visualizar información detallada acerca de una biblioteca específica

Visualizar la información detallada sobre un volumen denominado JJY008. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query libvolume jjy008 format=detailed
```

```

Nombre biblioteca: HPW3494
Nombre volumen: JJY008
Estado: Privado
Propietario: SUNSET
Última utilización: Datos
Elemento inicio:
Tipo dispositivo:
Limpiezas restantes:
Tipo de medio:

```

Descripciones de los campos

Nombre de biblioteca

El nombre de la biblioteca donde se encuentra el volumen de almacenamiento.

Nombre de volumen

El nombre del volumen de almacenamiento.

Estado

El estado del volumen de almacenamiento según el inventario de biblioteca. Si el estado es Privado, el volumen lo está utilizando IBM Spectrum Protect. Si el estado es Reutilizable), el volumen está disponible para ser utilizado.

Propietario

El servidor propietario del volumen, si el volumen es privado.

Última utilización

Tipo de datos del volumen. Este campo se aplica únicamente a los volúmenes en estado Privado. Para volúmenes de agrupación de almacenamiento, este campo muestra **Data**. Para los volúmenes de copia de seguridad de la base de datos (completa, incremental, de instantánea), este campo muestra **DbBackup**.

Elemento inicial

La dirección de elemento de la ranura de biblioteca que contiene el volumen.

Tipo de dispositivo

El tipo de dispositivo en el que se utiliza el volumen. Este campo sólo visualizará un valor para los volúmenes dados de alta en una biblioteca que tenga funciones de medios mixtas.

Limpiezas restantes

Para cartuchos de limpieza, el número de limpiezas restantes.

Tipo de medio

El tipo de medio que representa el volumen (por ejemplo, cinta de 8mm).

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY LIBVOLUME

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.

Mandato	Descripción
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

QUERY LICENSE (Visualizar información sobre licencias)

Utilice este mandato para visualizar la auditoría de licencias, los plazos de licencias y la información de conformidad.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query LICense-----<<
```

Parámetros

Ninguno.

Para visualizar la información sobre licencia, emita el mandato siguiente:

```
query license
```

Se visualiza la salida de ejemplo siguiente:

```
ANR2017I El administrador SERVER_CONSOLE ha emitido el mandato: QUERY LICENSE
          Última auditoría licencia: 10/17/2016 14:28:08
          Número de Data Protection para Oracle en uso: 0
            Número de Data Protection for
              Oracle en evaluación con opción a compra: 0
          Número de Data Protection for Microsoft SQL en uso: 0
            Número de Data Protection for
              Microsoft SQL en evaluación con opción a compra: 0
          Número de Data Protection for
            Microsoft Exchange en uso: 0
            Número de Data Protection for
              MS Exchange en evaluación con opción a compra: 0
          Número de TDP para Lotus Notes en uso: 12
          Número de TDP para Lotus Notes en evaluación con opción a compra: 0
          Número de Data Protection for Lotus Domino en uso: 0
            Número de Data Protection for
              Lotus Domino en evaluación con opción a compra: 0
          Número de TDP para Informix en uso: 1
          Número de TDP para Informix en evaluación con opción a compra: 0
            Número de TDP para SAP R/3 en uso: 0
          Número de TDP para SAP R/3 en evaluación con opción a compra: 0
            Número de TDP para ESS en uso: 0
          Número de TDP para ESS en evaluación con opción a compra: 0
            Número de TDP para ESS R/3 en uso: 0
          Número de TDP para ESS R/3 en evaluación con opción a compra: 0
            Número de TDP para EMC Symmetrix en uso: 0
          Número de TDP para EMC Symmetrix en evaluación con opción a compra: 0
```

Número de TDP para EMC Symmetrix R/3 en uso: 6
 Número de TDP para EMC Symmetrix R/3 en evaluación con opción a compra: 0
 Número de TDP para WAS en uso: 0
 Número de of TDP para WAS en evaluación con opción a compra: 0
 ¿Se está utilizando IBM Spectrum Protect for Data Retention?: No
 ¿Tiene licencia IBM Spectrum Protect for Data Retention?: Sí
 ¿Se está utilizando IBM Spectrum Protect Basic Edition?: Sí
 ¿Tiene licencia IBM Spectrum Protect Basic Edition?: Sí
 ¿Se está utilizando IBM Spectrum Protect Extended Edition?: No
 ¿Tiene licencia IBM Spectrum Protect Extended Edition?: Sí
 Cumplimiento licencia servidor: Válido

Descripciones de los campos

Última auditoría licencia

Especifica la fecha y hora en que se ha producido la última auditoría de licencia.

Número de Data Protection para Oracle en uso

Especifica el número de Data Protection para Oracle en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection para Oracle en evaluación con opción a compra

Especifica el número de Data Protection para Oracle que están en evaluación con opción a compra.

Número de Data Protection for Microsoft SQL en uso

Especifica el número de Data Protection for Microsoft SQL que se están utilizando. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection for Microsoft SQL en evaluación con opción a compra

Especifica el número de Data Protection for Microsoft SQL en evaluación con opción a compra.

Número de Data Protection for Microsoft Exchange en uso

Especifica el número de Data Protection for Microsoft Exchange que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection for Microsoft Exchange en evaluación con opción a compra

Especifica el número de Data Protection for Microsoft Exchange en evaluación con opción a compra.

Número de TDP para Lotus Notes en uso

Especifica el número de TDP para Lotus Notes que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de TDP para Lotus Notes en evaluación con opción a compra

Especifica el número de TDP para Lotus Notes que están en evaluación con opción a compra.

Número de Data Protection for Lotus Domino en uso

Especifica el número de Data Protection for Lotus Domino que se están utilizando. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection for Lotus Domino en evaluación con opción a compra

Especifica el número de Data Protection for Lotus Domino que están en evaluación con opción a compra.

Número de TDP para Informix en uso

Especifica el número de TDP para Informix que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de TDP para Informix con opción a compra

Especifica el número de TDP para Informix que están en evaluación con opción a compra.

Número de TDP para SAP R/3 en uso

Especifica el número de TDP para SAP R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

TDP para SAP R/3 de evaluación con opción a compra

Especifica el número de TDP para SAP R/3 que están en evaluación con opción a compra.

Número de TDP para ESS en uso

Especifica el número de TDP para ESS que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

TDP para ESS de evaluación con opción a compra

Especifica el número de TDP para ESS que están en evaluación con opción a compra.

Número de TDP para ESS R/3 en uso

Especifica el número de TDP para ESS R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

TDP para ESS R/3 de evaluación con opción compra

Especifica el número de TDP para ESS R/3 que están en evaluación con opción a compra.

Número de TDP para EMC Symmetrix en uso

Especifica el número de TDP para EMC Symmetrix que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

TDP para EMC Symmetrix de eval. con opción compra

Especifica el número de TDP para EMC Symmetrix que están en evaluación con opción a compra.

Número de TDP para EMC Symmetrix R/3 en uso

Especifica el número de TDP para EMC Symmetrix R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

TDP para EMC Symmetrix R/3 de eval. con opción compra

Especifica el número de TDP para EMC Symmetrix R/3 que están en evaluación con opción a compra.

Número de TDP para WAS en uso

Especifica el número de TDP para WAS que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de TDP de WAS de evaluación con opción a compra

Especifica el número de TDP para WAS que están en evaluación con opción a compra.

¿Se está utilizando IBM Spectrum Protect for Data Retention?

Especifica si IBM Spectrum Protect para retención de datos está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

¿Tiene licencia IBM Spectrum Protect for Data Retention?

Especifica si IBM Spectrum Protect para retención de datos tiene licencia.

¿Se está utilizando IBM Spectrum Protect Basic Edition?

Especifica si IBM Spectrum Protect Basic Edition está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

¿Tiene licencia IBM Spectrum Protect Basic Edition?

Especifica si IBM Spectrum Protect Basic Edition tiene licencia.

¿Se está utilizando IBM Spectrum Protect Extended Edition?

Especifica si IBM Spectrum Protect Extended Edition está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

¿Tiene licencia IBM Spectrum Protect Extended Edition?

Especifica si IBM Spectrum Protect Extended Edition tiene licencia.

Cumplimiento licencia servidor

Especifica si la licencia de servidor es válida.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY LICENSE

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY AUDITOCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra las estimaciones de las unidades de valor de procesador. Recuerde: El mandato QUERY PVUESTIMATE informa de las licencias proporcionando información de PVU para cada nodo para los dispositivos de servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

QUERY LOG (Visualizar información sobre el registro de recuperación)

Utilice este mandato para visualizar la información sobre las anotaciones de recuperación.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-Format----Standard----.
>>-Query LOG----->>
'-Format---+-Standard-+'
          '-Detailed-'
```

Parámetros

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información de resumen acerca de las anotaciones de recuperación

Visualizar información de resumen acerca de las anotaciones de recuperación. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query log
```

Espacio total (MB)	Espacio utilizado (MB)	Espacio libre (MB)
38,912	543.3	38,368.7

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: visualizar información detallada acerca de las anotaciones de recuperación

Visualizar información detallada sobre las anotaciones de recuperación. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query log format=detailed
```

```
Directorio anotaciones activas: /actlog
Espacio total(MB): 524.032
Espacio utilizado(MB): 3.517
Espacio libre (MB): 520.515
```

```
Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722
```

```
Directorio anotaciones archivado: /archlog
Tamaño total del sistema de archivos (MB): 603.751,82
Espacio utilizado en el sistema de archivos (MB): 80.642,30
Espacio libre en el sistema de archivos (MB): 523.109,52
Registro de archivado comprimido: Sí
```

```
Directorio anotaciones duplicadas: /mirrorlog
Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722
```

```
Directorio anotac. recuperación errores archivado: /archfaillog
Tamaño total del sistema de archivos (MB): 301.372,06
Espacio utilizado en el sistema de archivos (MB): 44.741,80
Espacio libre en el sistema de archivos (MB): 256.630,26
```

 Sistemas operativos Windows

Ejemplo: visualizar información detallada acerca de las anotaciones de recuperación cuando el registro duplicado y el registro de migración tras error de archivado no están definidos.

La salida de este mandato en sistemas Windows es diferente. Por ejemplo, la salida contiene espacios en blanco para el registro duplicado y el registro de migración tras error de archivado.

Visualizar información acerca de las anotaciones de recuperación cuando el registro duplicado y el registro de migración tras error de archivado no están definidos.

```
query log format=detailed
```

 Sistemas operativos Windows

```
Directorio de registro activo : d:\actlog
Espacio total(MB): 524.032
Espacio utilizado(MB): 3.517
Espacio libre (MB): 520.515

Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722

Directorio de registro activo : e:\archlog
Tamaño total del sistema de archivos (MB): 603.751,82
Espacio utilizado en el sistema de archivos (MB): 80.642,30
Espacio libre en el sistema de archivos (MB): 523.109,52
Registro de archivado comprimido: Sí

Directorio anotaciones duplicadas:
Tamaño total del sistema de archivos (MB):
Espacio utilizado en el sistema de archivos (MB):
Espacio libre en el sistema de archivos (MB):

Directorio de registro de recuperación de errores de archivado:
Tamaño total del sistema de archivos (MB):
Espacio utilizado en el sistema de archivos (MB):
Espacio libre en el sistema de archivos (MB):
```

Descripciones de los campos

Espacio total

Especifica el tamaño máximo de las anotaciones activas en megabytes.

Espacio utilizado

Especifica la cantidad de espacio de anotaciones activas utilizado en megabytes.

Espacio libre

Especifica la cantidad de espacio de anotaciones activas que no se utiliza para transacciones sin validar, en megabytes.

Tamaño total del sistema de archivos

Especifica el tamaño total del sistema de archivos, en megabytes.

Espacio utilizado en el sistema de archivos

Especifica la cantidad de espacio utilizado en el sistema de archivos, en megabytes.

Espacio libre en el sistema de archivos

Especifica la cantidad de espacio disponible en el sistema de archivos, en megabytes.

Registro de archivado comprimido

Especifica si los registros de archivado están comprimidos.

Directorio de anotaciones activas

Especifica la ubicación donde se guardan los archivos de anotaciones activas. Cuando cambie el directorio de anotaciones activas, el servidor moverá todas las anotaciones archivadas al directorio de anotaciones de archivado y todas las anotaciones activas a un nuevo directorio de anotaciones activas.

Directorio anotaciones duplicadas

Especifica la ubicación en la que se mantiene la duplicación de las anotaciones activas.

Directorio de anotaciones de recuperación de errores de archivado

Especifica la ubicación en la que el servidor guarda las anotaciones de archivado si las anotaciones no se pueden archivar en el directorio de anotaciones de archivado.

Directorio de anotaciones de archivado

Especifica la ubicación en la que el servidor puede archivar un archivo de anotaciones una vez finalizadas todas las transacciones representadas en dicho archivo de anotaciones.

QUERY MACHINE (Consultar información de máquina)

Utilice este mandato para visualizar información sobre una o varias máquinas. Puede utilizar esta información para recuperar máquinas cliente de IBM Spectrum Protect en caso de producirse un siniestro.

Atención: IBM Spectrum Protect no utiliza la información de ningún modo. Sólo está disponible para ayudar a planificar la recuperación ante siniestro de las máquinas cliente.

IBM Spectrum Protect visualiza la información de varias máquinas en el orden siguiente:

- Según la prioridad especificada.
- Dentro de una prioridad, según el nombre de ubicación y de máquina especificado.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----.  
>>-Query MACHine--+-+-----+-----+-----+----->  
                '-machine_name-' '-BUilding---edificio-'  
  
>--+-----+-----+-----+----->  
    '-FLoor---planta-' '-ROom---sala-'  
  
>--+-----+-----+-----+----->  
    '-PRIority---prioridad-' '-ADSMServer---+Yes-+-'  
                                '-No--'  
  
.Format---Standard-----.  
>--+-----+-----+-----+-----><  
    '-Format---+Standard-----+'  
        +-Detailed-----+  
        +-RECOVERYInstructions-+  
        '-CHaracteristics-----'
```

Parámetros

machine_name

Especifica el nombre de una o varias máquinas que se consultarán. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todas las máquinas que se ajustan a los criterios especificados.

BUilding

Especifica el nombre o número del edificio donde están las máquinas. Este parámetro es opcional. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

FLoor

Especifica el nombre o número de la planta donde están las máquinas. Este parámetro es opcional. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

ROom

Especifica el nombre o número de la sala donde están las máquinas. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

PRIority

Especifica el número de prioridad de las máquinas. Este parámetro es opcional.

ADSMServer

Especifica si la máquina contiene un servidor IBM Spectrum Protect. Este parámetro es opcional. El valor predeterminado es visualizar todas las máquinas que se ajustan a los demás criterios. Los valores posibles son:

Yes

La máquina contiene un servidor de IBM Spectrum Protect.

No

Las máquinas no contienen un servidor de IBM Spectrum Protect.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Visualiza información parcial sobre las máquinas.

Detailed

Visualiza toda la información sobre las máquinas.

RECOVERYInstructions

Sólo visualiza las instrucciones de recuperación de las máquinas. Esta opción sólo es válida cuando se consulta una máquina específica.

CHaracteristics

Sólo visualiza las características de las máquinas. Esta opción sólo es válida cuando se consulta una máquina específica.

Ejemplo: visualizar información acerca de una máquina específica

Visualizar información sobre la máquina denominada MACH1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query machine MACH1
```

Nombre máquina	Prioridad máquina	Edificio	Planta	Sala	Nodo	Nombre medio recuperación
MACH1	1	21	2	2929	VIRGINIA	RECMED1

Ejemplo: visualizar información detallada acerca de las máquinas que tienen prioridad 1

Visualizar información detallada para todas las máquinas con prioridad 1 situadas en la segunda planta del edificio 21. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query machine * building=21 floor=2 priority=1  
format=detailed
```

```
Nombre máquina: MACH1  
Prioridad máquina: 1  
Edificio: 21  
Planta: 2  
Sala: 2929  
¿Servidor?: Sí  
Descripción: Máquina del servidor de TSM  
Nombre nodo: VIRGINIA  
Nombre medio recuperación: RECMED1  
¿Características?: Sí  
¿Instrucciones recuperación?: Sí
```

Descripciones de los campos

Nombre de máquina

El nombre de la máquina.

Prioridad máquina

La prioridad de recuperación de la máquina.

Edificio

El edificio donde está situada la máquina.

Planta

La planta donde está situada la máquina.

Sala

La sala donde está situada la máquina.

¿Servidor?

Si la máquina contiene un servidor de IBM Spectrum Protect.

Descripción

La descripción de la máquina.

Nombre del nodo

Los nodos cliente de IBM Spectrum Protect asociados a esta máquina.

Nombre del medio de recuperación

Los medios de recuperación asociados a esta máquina.

¿Características?

Si el texto de las características de la máquina está almacenado en la base de datos.

¿Instrucciones de recuperación?

Especifica si el texto de instrucciones de recuperación de una máquina se almacena en la base de datos de IBM Spectrum Protect.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY MACHINE

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
UPDATE MACHINE	Cambia la información para una máquina.

QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)

Utilice este mandato para que se visualice información acerca de los volúmenes de agrupación de almacenamiento primaria y de copia de acceso secuencial que se han trasladado con el mandato MOVE MEDIA.

Clase de privilegio

Todos los administradores con privilegios de sistema o de operador pueden emitir este mandato, excepto si incluye el parámetro CMD. Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de almacenamiento sin restricciones o de sistema. Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES (el valor predeterminado), el administrador debe tener privilegio de sistema.

El mandato QUERY MEDIA solo muestra volúmenes con un valor ACCESS MODE de READONLY o READWRITE.

Sintaxis

```

>>-Query MEDia----->
      .-*-----
      '-nombre_volumen-'

>--STGpool-----nombre_agrupación----->
      .-Days----0----
      '-Days----días-'

>+-----+----->
|          .,-----|
|          V          |
|'-WHERESTATUS-----+FULL-----+-'
|          +-Filling-+
|          '-EMPTy---'

>+-----+----->
|'-WHEREACcEss-----+READWrite-+-'
|          '-READOnly--'

      .-Format----Standard-----
>+-----+----->
|'-Format-----Standard-+-'
|          +-Detailed-+
|          '-Cmd-----'

>+-----+----->
|'-WHEREStAtE-----+All-----+-'
|          +MOUNTABLEInlib-----+
|          '-MOUNTABLENotinlib-'

>+-----+----->
|'-WHEREOVFLocAtion-----ubicación-' '-Cmd-----"mandato"-

      .-APPend----No-----
>+-----+----->
|'-CMDFilename-----nombre_archivo-' '-APPend-----+No-+-'

```

Parámetros

nombre_volumen

Especifica el nombre del volumen de agrupación de almacenamiento de copia o primaria de acceso secuencial que se visualizará. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar el nombre. Todos los volúmenes que coincidan se considerarán para su proceso. Si no especifica este parámetro, se visualizarán todos los volúmenes definidos en la agrupación de almacenamiento especificada con el parámetro STGPOOL.

STGpool (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de copia o primaria de acceso secuencial que se utilizará para seleccionar los volúmenes para proceso. Puede utilizar caracteres comodín para especificar el nombre. Se procesarán todas las agrupaciones de almacenamiento que coincidan. Si la agrupación de almacenamiento especificada no está gestionada por una biblioteca automatizada, no se visualizará ningún volumen.

Days

Especifica el número de días que deben transcurrir después de que se haya leído o grabado el volumen, y antes de que el volumen se pueda seleccionar para procesarlo. Este parámetro es opcional. Puede especificar un número comprendido entre 0 y 9999. El valor predeterminado es 0. Para calcular el número de días transcurridos, se utiliza la fecha de última grabación o la fecha de última lectura del volumen, la que sea más reciente de las dos.

WHERESTATUs

Especifica que la salida de la consulta debe restringirse en función del estado del volumen. Este parámetro es opcional. Puede especificar varios estados en una lista si separa cada uno con una coma sin dejar espacios intercalados. Si no especifica un valor para este parámetro, se visualizarán todos los volúmenes de la agrupación de almacenamiento especificada, independientemente de su estado.

Los valores posibles son:

FULL

Especifica que se visualizarán los volúmenes con estado FULL.

FILLing

Especifica que se visualizarán los volúmenes con estado FILLING.

EMPTy

Especifica que se visualizarán los volúmenes con estado EMPTY.

WHEREACcEss

Especifica que la salida debe limitarse según la modalidad de acceso a volumen. Este parámetro es opcional. Si no especifica un valor para este parámetro, la salida no estará limitada según la modalidad de acceso.

Los valores posibles son:

READWrite

Especifica que se visualizarán los volúmenes con la modalidad de acceso READWRITE.

READOnly

Especifica que se visualizarán los volúmenes con la modalidad de acceso READONLY.

Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial para los volúmenes de agrupaciones de almacenamiento de acceso secuencial especificados.

Detailed

Especifica que se visualizará información completa para los volúmenes de agrupaciones de almacenamiento de acceso secuencial especificados.

Cmd

Especifica que se crean mandatos ejecutables para los volúmenes de agrupación de almacenamiento que se han procesado mediante el mandato QUERY MEDIA. Estos mandatos se encontrarán en el archivo que se ha especificado con el parámetro CMDFILENAME en el mandato QUERY MEDIA. Si desea que los mandatos sólo se visualicen en la consola, especifique una serie nula (""") para CMDFILENAME. Si se ha especificado FORMAT=CMD pero no se ha especificado ninguna serie de mandatos con el parámetro CMD, el mandato QUERY MEDIA no se ejecutará correctamente.

WHEREState

Especifica el estado de los volúmenes que se procesan. Este parámetro restringe el proceso a los volúmenes que tienen el estado especificado. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

All

Especifica que se consultan los volúmenes en todos los estados. Los estados válidos son: MOUNTABLEINLIB y MOUNTABLENOTINLIB.

MOUNTABLEInlib

Especifica que se consultan los volúmenes que actualmente están en el estado MOUNTABLEINLIB. Los volúmenes en estado MOUNTABLEINLIB están en la biblioteca, y en el local, contienen datos válidos y están disponibles para su proceso en el local.

MOUNTABLENotinlib

Especifica que se consultan los volúmenes que actualmente están en el estado MOUNTABLENOTINLIB. Los volúmenes en estado MOUNTABLENOTINLIB no están en la biblioteca, no contienen datos válidos y no están disponibles para el proceso en el local.



WHEREOVFLocation


Especifica la ubicación de desbordamiento de los volúmenes que se visualizarán. Este parámetro es opcional. Este parámetro restringe el proceso a los volúmenes que están en la ubicación especificada. La longitud máxima de la lista de la ubicación es de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco.

CMd

Especifica la creación de mandatos ejecutables. Encierre la especificación de mandatos entre comillas. La longitud máxima de la especificación del mandato ejecutable es de 255 caracteres. Este parámetro es opcional.

Para cada volumen que el mandato QUERY MEDIA procesa correctamente, el servidor graba los mandatos asociados en un archivo. Especifique el nombre de archivo con el parámetro CMDFILENAME.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica un nombre de archivo, el mandato generará un nombre de archivo predeterminado agregando la serie exec.cmds.media al directorio del servidor.

 Sistemas operativos Windows Si no especifica un nombre de archivo, el mandato generará un nombre de archivo predeterminado agregando la serie exec.cmd.media al directorio del servidor.

Recuerde:

1. Si el mandato escrito en el archivo sobrepasa los 255 caracteres, se divide en varias líneas y se agrega un carácter de continuación (+) a todas menos a la última línea. Puede que deba alterar el carácter de continuación en función de los requisitos del producto que ejecuta los mandatos.
2. Si se especifica un mandato ejecutable con un valor para FORMAT distinto de CMD, la serie del mandato se pasará por alto y el mandato QUERY MEDIA no grabará ninguna línea de mandatos.

Especifique una serie de mandatos y las variables de sustitución que convengan:

serie

Especifica la serie para crear un mandato ejecutable que procese el nombre de volumen y/o la ubicación del volumen. Puede especificar cualquier texto de formato libre para la serie. No utilice comillas intercaladas. Por ejemplo, la siguiente es una especificación válida de un mandato ejecutable:

```
cmd="checkin libvolume &vol"
```

La siguiente es una especificación no válida de un mandato ejecutable:

```
cmd="checkin libvolume "&vol""
```

sustitución

Especifica una variable para la que desea que el mandato QUERY MEDIA sustituya un valor. Las posibles variables de sustitución son:

&VOL

Sustituye el nombre de volumen por &VOL. Puede especificar caracteres en minúsculas, &vol. No debe especificar ni espacios ni blancos entre el signo & y VOL. Si existen espacios o blanco entre el ampersand y VOL, el mandato QUERY MEDIA los tratará como si fueran series y no se establecerá ninguna sustitución. Si no se especifica &VOL, no se establecerá ningún nombre de volumen en el mandato ejecutable.

&LOC

Sustituye que el volumen por &LOC. Puede especificar caracteres en minúsculas, &loc. No debe especificar ni espacios ni blancos entre el signo & y LOC. Si existen espacios o blanco entre el ampersand y LOC, el mandato QUERY MEDIA los tratará como si fueran series y no se establecerá ninguna sustitución. Si no se especifica &LOC, no se establecerá ningún nombre de ubicación en el mandato ejecutable.

&VOLDSN

Sustituye el nombre de archivo del volumen por &VOLDSN. Un ejemplo de nombre de archivo de volumen de cinta de una agrupación de almacenamiento que utiliza el prefijo definido IBM Spectrum Protect310 es IBM Spectrum

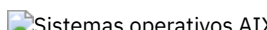
Protect310.BFS. Si no se especifica &VOLDSN, no se establecerá ningún nombre de archivo de volumen en el mandato ejecutable.


&NL

Sustituye un nuevo carácter de línea por &NL. Cuando se especifica &NL, el mandato QUERY MEDIA subdividirá el mandato en la posición en la que se encuentra &NL y no agregará ningún carácter de continuación. El usuario es el responsable de especificar el carácter de continuación correcto antes de &NL, si es necesario. El usuario también es el responsable de la longitud de la línea escrita. Si no se especifica &NL y el mandato sobrepasa los 255 caracteres, el mandato se dividirá en varias líneas y se agregará un carácter de continuación (+) a todas las líneas menos a la última.

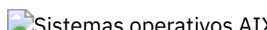
CMDFilename


Especifica el nombre de ruta totalmente calificado que contendrá los mandatos especificados con el parámetro CMD, cuando se especifica FORMAT=CMD. Este parámetro es opcional. La longitud máxima del nombre de archivo es de 1279 caracteres.

 Si especifica "" con el parámetro CMDFILENAME, el mandato QUERY MEDIA generará un nombre de archivo agregando "exec.cmds.media" al directorio del servidor. El directorio del servidor es el directorio de trabajo actual del proceso de servidor.

 Si especifica "" con el parámetro CMDFILENAME, el mandato QUERY MEDIA generará un nombre de archivo agregando "exec.cmd.media" al directorio del servidor. El directorio del servidor es el directorio de trabajo actual del proceso de servidor.

Si especifica una serie nula (""), los mandatos creados se visualizarán únicamente en la consola. Puede redirigir los mandatos visualizados a un archivo, utilizando los caracteres de redirección del sistema operativo (> o >>).

 Si el nombre de archivo no está especificado, el mandato generará un nombre de archivo predeterminado agregando la serie "exec.cmds.media" al directorio del servidor.

 Si el nombre de archivo no está especificado, el mandato generará un nombre de archivo predeterminado agregando la serie "exec.cmd.media" al directorio del servidor.

El mandato QUERY MEDIA asigna automáticamente el nombre de archivo especificado o generado. Si ya existe el nombre del archivo, el mandato QUERY MEDIA intentará utilizar éste y los datos existentes, si los hubiera, en el archivo que va a sobregrabarse. Puede especificar APPEND=YES para impedir que los datos existentes se sobregraben. Si el mandato QUERY MEDIA no se ejecuta correctamente después de haberse asignado el archivo de mandatos, el archivo no se suprimirá.

APPend

Especifica que se graba al principio o al final de los datos del archivo de mandatos. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se han de escribir datos desde el principio del archivo de mandatos. Si el archivo de mandatos dado ya existe, se sobregrabará el contenido.

Yes

Especifica que se agrega el archivo de mandatos grabando al final de los datos del archivo de mandatos.

Ejemplo: visualizar información acerca de una agrupación de almacenamiento de acceso secuencial específica

Visualizar todos los volúmenes completos o parcialmente completos que se encuentren en la agrupación de almacenamiento primaria de acceso secuencial, ARCHIVE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query media * stgpool=archive wherestatus=full, filling
```

Nombre volumen	Estado	Ubicación	Nombre biblioteca automatizada
TAPE01	Montable en biblioteca		LIB3494
TAPE03	Montable no en biblioteca	Room1234/Bldg31	
TAPE07	Montable en biblioteca		LIB3494
TAPE09	Montable no en biblioteca	Room1234/Bldg31	

Ejemplo: visualizar información acerca de una agrupación de almacenamiento de acceso secuencial con un prefijo específico

Visualizar detalladamente todos los volúmenes completos en estado MOUNTABLENOTINLIB para las agrupaciones de almacenamiento de acceso secuencial que tengan un nombre de prefijo de ONSITE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query media wherestate=mountablenotinlib stgpool=onsite*
wherestatus=full format=detailed
```

```
Nombre volumen: TAPE21
Estado: Montable no en biblioteca
Estado volumen: Lleno
Acceso: ReadOnly
Fecha última referencia: 30/01/98
Fecha/hora última actualización: 20/08/1996 13:29:02
Ubicación: Rm569/bldg31
Nombre agrupación almacenamiento: ONSITE.ARCHIVE
Nombre biblioteca automatizada:
```

```
Nombre volumen: TAPE22
Estado: Montable no en biblioteca
Estado volumen: Lleno
Acceso: ReadOnly
Fecha última referencia: 30/01/98
Fecha/hora última actualización: 20/08/1996 15:29:02
Ubicación: Rm569/bldg31
Nombre agrupación almacenamiento: ONSITE.ARCHIVEPOOL
Nombre biblioteca automatizada:
```

Ejemplo: generar mandatos para dar de alta

Generar los mandatos CHECKIN LIBVOLUME para los volúmenes llenos y parcialmente llenos que se encuentran en la agrupación de almacenamiento primaria ONSITE.ARCHIVE y que están almacenados en la ubicación de desbordamiento Room 2948/Bldg31.

```
query media * stgpool=onsite.archive format=cmd
wherestatus=full,filling wherestate=mountablenotinlib
whereovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

El mandato QUERY MEDIA que ha creado los mandatos ejecutables CHECKIN LIBVOLUME en /tsm/move/media/checkin.vols, que puede ejecutarse emitiendo el mandato MACRO con /tsm/move/media/checkin.vols como nombre de la macro.

```
checkin libvol lib3494 TAPE04 status=private
checkin libvol lib3494 TAPE13 status=private
checkin libvol lib3494 TAPE14 status=private
```

Descripciones de los campos

Nombre de volumen

Especifica el nombre del volumen de agrupación de almacenamiento de acceso secuencial primaria.

Estado

Especifica el estado del volumen.

Estado volumen

Especifica el estado del volumen.

Acceso

Especifica la modalidad de acceso del volumen.

Fecha última referencia

Especifica la fecha de la última grabación o de la última lectura del volumen, la que sea más reciente.

Fecha/hora última actualización

Especifica la fecha y la hora en que se ha actualizado por última vez el volumen.

Ubicación

Especifica donde se almacena el volumen. Si se expulsa el volumen de la biblioteca y su ubicación no se ha especificado ni definido, se visualizará un signo de interrogación (?) para la ubicación.

Nombre de la agrupación de almacenamiento

Especifica el nombre de la agrupación de almacenamiento de acceso secuencial donde está definido el volumen.

Biblioteca automatizada

Especifica el nombre de la biblioteca automatizada si el volumen está en la biblioteca.

Mandatos relacionados

EMPLOYEE- _RECORDS	ACTIVE	ACTIVEFI- LES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE- _RECORDS	HOLIDAY	ACTIVEFI- LES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE- _RECORDS	HOLIDAY	FILEHIST- ORY	No	Clase de gestión de prueba modificada
EMPLOYEE- _RECORDS	VACATION	ACTIVEFI- LES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE- _RECORDS	VACATION	FILEHIST- ORY	No	Clase de gestión de prueba modificada
PROG1	SUMMER	MCLASS1	No	Clase de gestión de soporte técnico
PROG2	SUMMER	MCLASS1	No	Clase de gestión de soporte técnico
STANDARD	ACTIVE	STANDARD	Sí	Clase gestión predeterminada instalada
STANDARD	STANDARD	STANDARD	Sí	Clase gestión clase de gestión

Para visualizar información sobre las clases de gestión de un dominio de políticas específico, por ejemplo el dominio ENGPOLDOM, emita el mandato siguiente:

```
query mgmtclass engpoldom * *
```

Ejemplo: visualizar información detallada acerca de una clase de gestión específica

Consultar la clase de gestión ACTIVEFILES que se ha asignado al juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS. Crear la salida en formato detallado. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query mgmtclass employee_records vacation
activefiles format=detailed

Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre juego políticas: VACATION
Nombre clase gestión: ACTIVEFILES
¿Clase de gestión predeterminada?: Sí
Descripción: Clase de gestión
predeterminada
instalada

Técnica gestión espacio: Ninguna
¿Migrar automáticamente al no utilizar?: 0
¿Migración requiere copia de seguridad?: Sí
Destino migración: SPACEMGPOOL
Última actualización por (administrador): $$CONFIG MANAGER$$
Fecha/hora última actualización: 31/05/1996 13:15:45
Perfil gestión: EMPLOYEE
Cambios pendientes: Sí
```

Descripciones de los campos

Nombre de dominio de políticas

El dominio de políticas.

Nombre de juego de políticas

El juego de políticas.

Nombre clase gestión

La clase de gestión.

¿Clase gestión predeterminada?

Si la clase de gestión es la clase de gestión predeterminada para el juego de políticas.

Descripción

La descripción de la clase de gestión.

Técnica gestión espacio

La técnica de gestión de espacio de la clase de gestión, para los clientes de IBM Spectrum Protect for Space Management.

Migrar automáticamente al no utilizar

El número de días que deben transcurrir desde que se accedió por última vez a un archivo hasta que pueda seleccionarse para la migración automática mediante clientes IBM Spectrum Protect for Space Management.

¿Migración requiere copia seguridad?

Si debe existir una versión de copia de seguridad de un archivo para que pueda migrarse mediante clientes IBM Spectrum Protect for Space Management.

Destino migración

La agrupación de almacenamiento que es el destino de los archivos migrados mediante clientes IBM Spectrum Protect for Space Management.

Última actualización por (administrador)

El administrador o el servidor que ha actualizado por última vez la clase de gestión. Si este campo contiene \$\$CONFIG_MANAGER\$\$, la clase de gestión se asocia a un dominio que el gestor de configuración gestiona.

Fecha/hora última actualización

La fecha y la hora en que se ha definido o actualizado por última vez la clase de gestión.

Perfil de gestión

El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de esta clase de gestión.

Cambios pendientes

Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY MGMTCLASS

Mandato	Descripción
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)

Utilice este mandato para visualizar información acerca de los valores de supervisión de alertas y de estado del servidor.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query MONITORSEttings-----<<
```

Visualizar valores de supervisión

Visualizar detalles sobre los valores de supervisión. Para obtener información detallada, consulte Descripciones de los campos.

```
query monitorsettings
```

Ejemplo de salida:

```
Estado de supervisión: Activo
Intervalo de renovación de estado (minutos): 5
Retención de estado (horas): 48
Alertas de mensajes del supervisor: Activo
Intervalo de actualización de alertas (min.): 10
Alerta por correo electrónico: Activo
Enviar resumen de alertas a administradores: Activo
Alerta desde dirección de correo electrónico: DJADMIN@MYDOMAIN.COM
Host SMTP de alerta: DJHOST.MYDOMAIN.COM
Puerto SMTP de alerta: 25
Duración de alerta activa (min.): 480
Duración de alerta inactiva (min.): 480
Duración de alerta cerrada (min.): 60
Admin. supervisión: ADMIN
Grupo supervisado: MONGROUP
```

```
    Servidores supervisados: SERVER2
Intervalo en peligro para aplicaciones: 24
¿Se han omitido archivos como en peligro para aplicaciones?: Sí
Intervalo en peligro para máquinas virtuales: 24
¿Se han omitido archivos como en peligro para máquinas virtuales?: Sí
Intervalo en peligro para sistemas: 24
¿Se han omitido archivos como en peligro para sistemas?: Sí
Repositorio de despliegue: /source/packages/deploy
Máximo de paquetes de despliegue: 4
Gestor de paquetes de despliegue: Activado
```

Descripciones de los campos

Supervisar estado

Especifica si la supervisión de alertas en el servidor está habilitada o inhabilitada.

Intervalo de renovación de estado (minutos)

Especifica el número de minutos entre los intervalos de tiempo que el servidor de supervisión recopila datos de evento.

Retención de estado (horas)

Especifica el número de horas que se retienen los indicadores de supervisión de estado.

Alertas de mensaje del supervisor

Especifica si se envían las alertas a los administradores por correo electrónico

Intervalo de actualización de alerta (minutos)

Especifica el periodo de tiempo, en minutos, que el supervisor de alertas espera antes de que se actualice o borre la alerta en el servidor.

Alertas en correo electrónico

Especifica si se envían las alertas a los administradores por correo electrónico

Enviar resumen de alertas a los administradores

Especifica los administradores que recibirán un resumen de las alertas existentes en el servidor por correo electrónico.

Alertas desde dirección de correo electrónico

Especifica la dirección de correo electrónico del remitente.

Host SMTP de alertas

Especifica el servidor de correo del host de protocolo simple de transferencia de correo (SMTP) que se utilizará para enviar las alertas.

Puerto SMTP de alertas

Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.

Duración activa de alerta (minutos)

Especifica el tiempo, en minutos, que una alerta permanece activa.

Duración inactiva de alerta (minutos)

Especifica el tiempo, en minutos, en que la alerta estará inactiva.

Duración cerrada de alerta (minutos)

Especifica el tiempo, en minutos, que una alerta permanece cerrada antes de que se suprima del servidor.

Administración de supervisión

Especifica el nombre del administrador de supervisión que se utiliza para conectarse a los servidores del grupo supervisado.

Grupo supervisado

Especifica el nombre del grupo de servidores supervisados.

Servidores supervisados

Especifica los nombres de los servidores del grupo de servidores supervisados. Los valores de supervisión pueden ser diferente en cada servidor supervisado. Si es así, emita el mandato de consulta para cada servidor para visualizar los valores de supervisión.

Intervalo de en riesgo para aplicaciones

Especifica el intervalo de tiempo, en horas, que un cliente de aplicaciones puede no registrar actividad antes de que se considere en peligro.

¿Archivos omitidos como en riesgo para aplicaciones?

Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.

Intervalo de en riesgo para máquinas virtuales

Especifica el intervalo de tiempo, en horas, que un cliente virtual puede no registrar actividad antes de que se considere en peligro.

¿Archivos omitidos como en riesgo para máquinas virtuales?

Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.

Intervalo de en riesgo para sistemas

Especifica el intervalo de tiempo, en horas, que un cliente de sistemas puede no registrar actividad antes de que se considere en peligro.

¿Archivos omitidos como en riesgo para sistemas?

Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.

Repositorio de despliegue

Especifica la ubicación donde se descargan los paquetes de despliegue del cliente, y la ubicación de los volúmenes de almacenamiento que se utilizan para los paquetes de despliegue del cliente.

Máximo de paquetes de despliegue

Especifica el número máximo de paquetes de despliegue de cliente que se almacenan en el repositorio de despliegue para cada versión del producto.

Gestor de despliegue de paquetes

Especifica si el gestor de paquetes de despliegue consulta el sitio FTP para obtener nuevos paquetes de despliegue y los descarga cuando están disponibles.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY MONITORSETTINGS

Mandato	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	Suprime un servidor de un grupo de servidores.
DELETE SERVER (Suprimir una definición de servidor)	Suprime la definición de un servidor.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET DEPLOYREPOSITORY (Establece la vía de acceso de descarga para los paquetes de despliegue del cliente)	Especifica la ubicación donde se descargan los paquetes de despliegue del cliente.
SET DEPLOYMAXPKGS (Establecer el número máximo de paquetes de despliegue del cliente para almacenar)	Especifica el número máximo de paquetes de despliegue de cliente que se descargarán y almacenarán en el servidor.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

QUERY MONITORSTATUS (Consultar el estado de supervisión)

Utilice este mandato para visualizar mensajes de estado que están dentro del periodo de retención de estado definido.

Puede limitar la salida a un estado especificado, por ejemplo sólo los mensajes con un estado de activo. Si no especifica ningún parámetro, se visualizan todos los mensajes.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-Format-----Standard-----.  
>>-Query MONITORStatus--+-+-----+----->
```


Ejemplo de salida:

```
Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
```

Visualizar valores de supervisión

Visualizar detalles acerca del estado de supervisión.

```
query monitorstatus f=d type=active
```

Salida del ejemplo:

```
Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
Detalles de elemento:
Sugerencia de reparación principal:
Primera sugerencia de reparación alternativa:
Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
Detalles de elemento:
Sugerencia de reparación principal:
Primera sugerencia de reparación alternativa:
Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
Detalles de elemento:
Sugerencia de reparación principal:
Primera sugerencia de reparación alternativa:
```

Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
Detalles de elemento:
Sugerencia de reparación principal:
Primera sugerencia de reparación alternativa:
Segunda sugerencia de reparación alternativa:

Descripciones de los campos

Nombre del servidor
El nombre del servidor.

Fecha de la actividad
Fecha y hora a las que se notificó la última actividad.

Nombre de actividad
Nombre de la actividad.

Nombre de elemento
Nombre del elemento.

Valor numérico de elemento
Valor numérico del elemento.

Valor de serie de elemento
Valor de serie del elemento.

Estado de elemento
Estado del elemento.

Detalles de elemento
Información detallada del elemento.

Sugerencia de reparación principal
Sugerencia de reparación principal.

Sugerencia principal de reparación alternativa
Sugerencia de reparación en caso de que la sugerencia principal no sea la adecuada.

Sugerencia secundaria de reparación alternativa
Sugerencia de reparación en caso de que la sugerencia principal y la primera alternativa no sean adecuadas.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY MONITORSTATUS

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)

Utilice este mandato para visualizar información sobre el estado de uno o varios volúmenes de acceso secuencial que están montados.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----.  
>>-Query MOUNT----->  
    '-nombre_volumen-'  
  
.-Format----Standard----.  
>----->  
    '-Format----Standard-+-'  
    '-Detailed-'
```

Parámetros

nombre_volumen

Especifica el nombre del volumen de acceso secuencial montado. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado es todos los volúmenes montados.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: obtener una lista de todos los volúmenes secuenciales montados

Visualizar información acerca de todos los volúmenes de medios secuenciales montados.

```
query mount
```

Sistemas operativos AIX

```
ANR8330I El volumen 3590 D6W992 está montado R/O  
en la unidad RMT1 (/dev/rmt1), estado: EN USO.  
ANR8334I 1 volúmenes encontrados.  
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W  
en la unidad 8MM.1 (/dev/mt0), estado: DESMONTÁNDOSE.  
ANR8334I 1 volúmenes encontrados.
```

Sistemas operativos Linux

```
ANR8330I El volumen 3590 D6W992 está montado R/O  
en la unidad RMT1/dev/IBMTape1, estado: EN USO.  
ANR8334I 1 volúmenes encontrados.  
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W  
en la unidad 8MM.1 (/dev/tmscsi/mt0), estado: DESMONTÁNDOSE.  
ANR8334I 1 volúmenes encontrados.
```

Sistemas operativos Windows

```
ANR8330I El volumen 3590 D6W992 está montado R/O  
en la unidad RMT1 (/dev/rmt1), estado: EN USO.  
ANR8334I 1 volúmenes encontrados.  
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W  
en la unidad 8MM.1 (mt3.0.0.0), estado: DESMONTÁNDOSE.  
ANR8334I 1 volúmenes encontrados.
```

Recuerde:

1. Si el estado de un volumen es lleno o si su modalidad de acceso es de sólo lectura (R/O), la modalidad de montaje del volumen es R/O. Para determinar el estado y la modalidad de acceso de un volumen, emita el mandato QUERY VOLUME FORMAT=DETAILED. Si se puede grabar en un volumen (es decir, el estado es llenando o vacío), la modalidad de montaje del volumen es Lectura/Grabación (R/W), aunque únicamente se esté leyendo.
2. En una agrupación de almacenamiento que está asociada con el tipo de dispositivo FILE o CENTERA, el servidor puede realizar varios accesos de lectura simultáneos y un único acceso de grabación al mismo volumen. Como resultado de ello, un volumen de una agrupación de almacenamiento con el tipo de dispositivo FILE o CENTERA puede aparecer montado más de una vez.
3. anr8448i en el mensaje, el nombre de la unidad se muestra como `unknown` para los volúmenes del tipo de dispositivo FILE con una clase de dispositivo no compartida. La razón es que no hay ninguna unidad asociada con los volúmenes; los nombres de unidades se muestran en la biblioteca basada en archivos.
4. Si emite el mandato QUERY MOUNT mientras la unidad se está limpiando, la salida del mandato continuará mostrando el estado `DISMOUNTING` para el volumen desmontado hasta que se complete la limpieza.

Ejemplo: visualizar información detallada sobre los volúmenes secuenciales montados

Visualice detalles sobre los volúmenes montados.

```
query mount format=detailed
```

```
ANR2017I El administrador SERVER_CONSOLE ha emitido el mandato: QUERY
Formato MOUNT=detallado
ANR8487I El punto de montaje de la clase de dispositivo FILE está esperando
a que se complete
el montaje del volumen -- servidor propietario: SERVER1, estado: EN ESPERA DE VOLUMEN
(sesión: 0, proceso: 1).
ANR8488I El volumen LTO 015005L4 está montado para L/G en la unidad IBMVTLL1
(/dev/rmt37) -- servidor
propietario: SERVER1, estado: EN USO (sesión: 0, proceso: 2).
ANR8486I El punto de montaje de la clase de dispositivo FILE está reservado -- servidor
propietario: SERVER1,
estado: RESERVADO (sesión: 5, proceso: 0).
ANR8334I          3 coincidencias encontradas
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY MOUNT

Mandato	Descripción
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
REPLY	Permite que una petición siga procesándose.

QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)

Utilice este mandato para visualizar información acerca de los objetos de imagen de sistema de archivos de los que se ha efectuado una copia de seguridad para un nodo NAS y un espacio de archivos específicos. Sólo puede emplear este mandato para visualizar los objetos de los que se ha hecho copia de seguridad para un nodo NAS mediante NDMP.

El servidor muestra todos los objetos coincidentes, las fechas en las que se ha efectuado una copia de seguridad de esos objetos e información sobre una tabla de contenido (TOC) para el objeto.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query NASBackup--nombre_nodo--nombre_espacioarchivos----->
.-BEGINDate-----TODAY - 7-. .-BEGINTime-----00:00:00-.
>--+-----+-----+-----+-----+-----+-----+-----+----->
'-BEGINDate-----fecha-----' '-BEGINTime-----hora-----'
.-ENDDate-----TODAY-. .-ENDTime-----23:59:59-.
```

```

>-----+-----+-----+-----+----->
'-ENDDate----fecha-' '-ENDTime----hora-----'

.-TYPE----BACKUPImage-----
>-----+-----+-----+-----+-----<
'-TYPE----+BACKUPImage-+-'
'-SNAPMirror--'

```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo NAS para el que se visualizan los objetos de copia de seguridad. No puede utilizar caracteres comodín para especificar este nombre.

nombre_espacio_archivos (Obligatorio)

Especifica el nombre del espacio de archivos para el que se visualizan los objetos de copia de seguridad. Puede utilizar caracteres comodín para especificar este nombre.

BEGINDate

Especifica la fecha inicial para seleccionar los objetos de copia de seguridad que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados en la fecha especificada o a partir de ella. El valor predeterminado es siete días antes de la fecha actual. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la hora y la fecha. Este parámetro es opcional.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/2002
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para visualizar la información sobre los mensajes creados una semana atrás, puede especificar BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial para seleccionar los objetos de copia de seguridad que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados a la hora especificada o a partir de ella. Este parámetro es opcional. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada para BEGINDATE.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, el servidor visualizará los registros que tengan la hora 12:00 o posterior en la fecha inicial.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00. Si emite este mandato a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, el servidor visualiza los objetos de imágenes con la hora 5:30 o posterior en la fecha inicial.

ENDDate

Especifica la fecha final utilizada para seleccionar los objetos que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados en la fecha especificada o antes de ella. Este parámetro es opcional. El valor predeterminado es la fecha actual. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha finales. Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/2002
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para visualizar la información creada hasta ayer, puede especificar ENDDATE=TODAY-1, o simplemente, ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final utilizada para seleccionar los objetos que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados a la hora especificada o antes de ella. Este parámetro es opcional. El valor predeterminado son las 23:59:59. Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha. Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, el servidor visualiza los objetos de imágenes con la hora 12:00 o posterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, el servidor visualizará los objetos de imágenes con la hora 5:30 o posterior en la fecha final especificada.

TYPE

Especifica el tipo de imágenes de copia de seguridad NDMP sobre el que desea visualizar información. El valor predeterminado para este parámetro es BACKUPIIMAGE. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser

específicos para un servidor de archivos determinado. Los valores posibles son:

BACKUPImage

Especifica que la salida sólo debe mostrar las imágenes diferenciales y básicas estándares de NAS. Este es el valor predeterminado para este parámetro.

SNAPMirror

Especifica si ha de visualizarse información sobre las imágenes NetApp SnapMirror. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos. Una imagen SnapMirror solo puede restaurarse en un sistema de archivos que se haya preparado como volumen de destino SnapMirror. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más información. Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM N-Series.

Ejemplo:

Emitir el mandato QUERY NASBACKUP para que se visualice información acerca de un nodo, nas1, y un espacio de archivos, /vol/vol1.

```
query nasbackup nas1 /vol/vol1
```

Node Name	Filespace Name	Object Type (MB)	Object Size (MB)	Creation Date Contents	Has Table of Contents (TOC)	Mgmt Class Name	Image Storage Pool
NAS1	vol/vol1	Imag.	1050.5	10/22/2002 10:50:57	YES	DEFAULT	NASBACKUPS
NAS1	vol/vol1	Imagen diferenc.	9.1	10/22/2002 11:03:21	YES	DEFAULT	NASBACKUPS
NAS1	vol/vol1	Imag. compl.	1050.5	10/22/2006 10:43:00	YES	STANDARD	FILEPOOL
NAS1	vol/vol1	Imagen diferencial	9.1	10/25/2006 11:53:21	YES	STANDARD	FILEPOOL

Ejemplo:

Emita el mandato QUERY NASBACKUP para mostrar información sobre todas las imágenes de NetApp SnapMirror to Tape para un nodo, nas2, y para un espacio de archivos, /vol/vol2.

```
query nasbackup nas2 /vol/vol2 type=snapmirror
```

Nombre de nodo	Nombre de espacio de archivos	Tipo de objeto	Tamaño de objeto (MB)	Fecha de creación	Nombre clase gestión de imagen	Nombre de agrupac. almacen.
NAS2	vol/vol2	SnapMirror	1050.5	04/02/2008 10:50:57	ESTÁNDAR	MIAGRUPACIÓN
NAS2	vol/vol2	SnapMirror	1450.5	04/02/2008 11:03:21	ESTÁNDAR	MIAGRUPACIÓN

Descripciones de los campos

Nombre del nodo

El nombre del nodo cliente.

Nombre de espacio de archivos

Nombre del espacio de archivos.

Tipo de objeto

Tipo de objeto del que se ha realizado una copia de seguridad.

Tamaño de objeto (MB)

Tamaño del objeto en megabytes.

Fecha de creación

Fecha de creación de la copia de seguridad.

Nombre clase gestión

El nombre de la clase de gestión.

Nombre de agrupación de almacenamiento de imágenes

Nombre del almacenamiento donde se encuentra la copia de seguridad.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY NASBACKUP

- Any
Especifica todos los tipos de nodo.
- Client
Especifica los nodos cliente que son clientes de copia de seguridad/archivado, clientes IBM Spectrum Protect for Space Management o clientes de aplicación.
- NAS
Especifica nodos NAS.
- Server
Especifica los nodos cliente que son otros servidores de .
- Authentication
Especifica el método de autenticación de contraseña para el nodo.
- Local
Muestra aquellos nodos que se autentican en el servidor de IBM Spectrum Protect.
- LDap
Muestra aquellos nodos que se autentican en el servidor de directorios LDAP. La contraseña del nodo es sensible a las mayúsculas/minúsculas.

Ejemplo: visualizar información acerca de los nodos de cliente registrados

Visualizar información sobre todos los nodos de cliente registrados.

```
query node
```

Nombre	Platafor.	Nombre nodo	Días desde dominio	Días desde último políticas	Bloqueo asignación acceso	contraseña
CLIENT1	AIX	STANDARD	6	6	No	
GEORGE	AIX	STANDARD	1	1	No	
JANET	AIX	STANDARD	1	1	No	
JARED	Linux86	STANDARD	1	1	No	
JOE2	Mac	STANDARD	<1	<1	No	
TOMC	WinNT	STANDARD	1	1	No	

Ejemplo: visualizar información detallada acerca de un nodo cliente

Visualizar información completa sobre el nodo cliente llamado Joe.



```
query node joe format=detailed
```

```

Nombre nodo: JOE
Plataforma: WinNT
Nivel SO cliente: 4.00
Versión cliente: Versión 5, Release 4, Nivel 0.0
Versión de la aplicación: Versión 6, Release 4, Nivel 0.4
Nombre dominio políticas: STANDARD
Fecha/hora último acceso: 09/24/2012 18:55:46
Días desde último acceso: 6
Fecha/hora asignación contraseña: 24/09/2012 18:26:43
Días desde asignación contraseña: 6
Número conexiones no válidas: 0
Bloqueo: No
Contacto:
Compresión: Cliente
¿Supresión copias archivadas?: Sí
¿Supresión copias seguridad?: No
Fecha/hora de inscripción: 24/09/2012 18:26:43
Inscrito por administrador: SERVER_CONSOLE
Último método comunicación utilizado: Tcp/Ip
Bytes recibidos última sesión: 108,731
Bytes enviados última sesión: 698
Duración de última sesión: 0,00
Porcentaje de esperas desocupado última sesión: 0,00
Porcentaje de Método comunicaciones última sesión: 0.00
Porcentaje de esperas medio última sesión: 0,00
Conjunto opciones:
URL: http://joe.host.name:1581
Tipo de nodo: Cliente
Período caducidad contraseña: 60
¿Mantener punto de montaje?: No

```

Número máximo de puntos de montaje permitidos: 2
 Cambiar nombre de espacio de archivos automáticamente: No
 Protocolo de validación: No
 Nombre TCP/IP:
 Dirección TCP/IP: 9.11.153.39
 ID exclusivo global: 11.9c.54.e0.8a.b5.11.d6.b3.c3.00.06.29.45.c1
 Archivos máximos en grupo de transacción: 0
 Ruta de grabación de datos: ANY
 Ruta de lectura de datos: ANY
 Iniciación de sesión: ClientOrServer
 Dirección de alto nivel:
 Dirección de bajo nivel: 1501
 Nombre de grupo de proximidad:
 Nodo proxy destino:
 Agente de nodo proxy:
 Grupos de nodo:
 Dirección de correo electrónico:
 Eliminación de duplicados: ServerOnly

 Sistemas operativos AIX  Sistemas operativos Linux Usuarios permitidos para realizar copias de seguridad: ALL

Estado de réplica: activado
 Modalidad de réplica: Enviar
 Regla de réplica de copia de seguridad: DEFAULT
 Regla de réplica de archivado: ALL_DATA
 Regla de réplica de gestión de espacio: Ninguna
 Servidor primario de réplica: PRODSERVER1
 Última réplica en servidor: DRSERVER1
 Nombre de sistema operativo cliente: WIN: Windows XP
 Arquitectura de procesador de cliente: x86
 Productos de cliente instalados: WIN, FCM, VE
 Versión de destino de cliente: Versión 6, Release 2, Nivel 0.0
 Autenticación: Local
 SSL necesario: No
 Session Security: Strict
 Método de transporte: TLS 1.2
 Dividir objetos grandes: Sí
 Tipo de riesgo: Intervalo predeterminado
 Intervalo de riesgo:
 URL de utilidad:
 Recuperación de duplicación de archivos dañados: sí
 Fuera de servicio:
 Fecha de fuera de servicio:

Descripciones de los campos

Nombre del nodo

El nombre del nodo cliente.

Plataforma

Sistema operativo del nodo de cliente existente la última vez que el nodo de cliente contactó con el servidor. El signo de interrogación (?) se visualizará hasta que el nodo de cliente acceda al servidor por primera vez e informe acerca de su tipo de sistema operativo.

Nivel SO cliente

Nivel del sistema operativo para el cliente existente la última vez que el nodo de cliente contactó con el servidor.

Versión del cliente

La versión del cliente instalado en el nodo cliente.

Este campo no se aplica a los nodos NAS.

Versión de la aplicación

Versión del cliente de Data Protection for VMware.

Nombre de dominio de políticas

El dominio de políticas asignado del nodo de cliente.

Fecha/hora último acceso

La última fecha y hora en que el nodo cliente ha accedido al servidor.

Días desde último acceso

Número de días que han transcurrido desde la última vez que el nodo de cliente accedió al servidor.

Fecha/hora asignación contraseña

Fecha y hora del establecimiento de la contraseña del nodo de cliente.

Días desde asignación contraseña

Número de días que han transcurrido desde que se estableció la contraseña para el nodo de cliente.

Contador de conexiones no válidas

Número de intentos de inicio de sesión no válidos que se han realizado desde el último inicio de sesión satisfactorio. Este número puede ser distinto de cero solo cuando el límite de contraseña no válida (SET INVALIDPWLIMIT) es mayor que cero. Cuando el número de intentos no válidos es igual al límite establecido por el mandato SET INVALIDPWLIMIT, el nodo queda bloqueado respecto al sistema.

Bloqueo

Si el nodo de cliente está bloqueado en IBM Spectrum Protect.

Contacto

Cualquier información de contacto del nodo cliente.

Compresión

Si la compresión está activada en el nodo cliente.

Este campo no se aplica a los nodos NAS.

¿Supresión copias archivadas?

Si el nodo cliente puede suprimir sus propias copias archivadas.

¿Supresión copias seguridad?

Si el nodo cliente puede suprimir sus propias copias archivadas.

Fecha/hora registro

La fecha y la hora en que se ha inscrito el nodo cliente.

Registrado por administrador

El nombre del administrador que ha inscrito el nodo cliente.

Último método comunicación utilizado

El método de comunicación que ha utilizado por última vez el nodo cliente para contactar con el servidor.

Bytes recibidos última sesión

El número de bytes que ha recibido el servidor durante la última sesión del nodo cliente.

Este campo no se aplica a los nodos NAS.

Bytes enviados última sesión

El número de bytes enviados al nodo cliente.

Este campo no se aplica a los nodos NAS.

Duración última sesión

Cuánto tiempo ha durado la última sesión del nodo de cliente, en segundos.

Este campo no se aplica a los nodos NAS.

Porcentaje de esperas desocupado última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente no ha estado ejecutando ninguna función.

Este campo no se aplica a los nodos NAS.

Porcentaje de Método comunicaciones última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando una respuesta del servidor.

Este campo no se aplica a los nodos NAS.

Porcentaje de esperas soporte última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando que se montara un volumen extraíble.

Este campo no se aplica a los nodos NAS.

Conjunto de opciones

El nombre del conjunto de opciones del cliente.

URL

El URL del cliente web de IBM Spectrum Protect que está configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

Tipo de nodo

El tipo de nodo cliente. Son posibles los valores siguientes:

- Cliente: un cliente de archivado y copia de seguridad, un cliente de IBM Spectrum Protect for Space Management o un cliente de aplicaciones
- Servidor: un servidor de IBM Spectrum Protect
- NAS: servidor de archivos de almacenamiento conectado a red

Período de caducidad de contraseña

El período de caducidad de contraseña del nodo de cliente.

¿Mantener punto de montaje?

Si el nodo de cliente retiene un punto de montaje durante una sesión.

Número máximo de puntos de montaje permitidos

El número de puntos de montaje que un nodo de cliente puede utilizar en el servidor para las operaciones de migración de IBM Spectrum Protect for Space Management y de copia de seguridad y archivado. Este parámetro no se aplica a los nodos con un tipo NAS o SERVER. Si un nodo de cliente se ha registrado en un servidor de la Versión 3.7 o posterior, el valor estará comprendido entre 0 y 999, en función del valor que se ha establecido con el parámetro MAXNUMMP del mandato REGISTER NODE. Si el nodo cliente se ha registrado en versiones anteriores del servidor y el parámetro MAXNUMMP no se ha establecido explícitamente con el mandato UPDATE NODE, el valor se establece en NOLIMIT. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos de las operaciones de almacenamiento de datos simultáneas del mismo nodo de cliente. Esta evaluación puede impedir que las operaciones de almacenamiento de datos adquieran puntos de montaje.

Cambiar nombre de espacio de archivos automáticamente

Si IBM Spectrum Protect solicita al cliente que redetermine los espacios de archivos cuando el sistema cliente se actualiza a un cliente que admite Unicode. Este campo sólo es válido para los sistemas cliente que utilizan los sistemas operativos Windows, Macintosh OS X o NetWare.

Protocolo de validación (en desuso)

Si el cliente tiene activada la validación de datos. Si el cliente tiene activada la validación, este campo especifica si IBM Spectrum Protect valida sólo los datos del archivo o todos los datos, incluidos los metadatos del archivo. Puede habilitar la validación de datos con los mandatos REGISTER NODE o UPDATE NODE. Este campo está en desuso.

Nombre TCP/IP

Nombre de host del nodo cliente existente la última vez que el nodo cliente contactó con el servidor. El campo se deja vacío si el software de cliente no admite la notificación de esta información al servidor.

Dirección TCP/IP

Dirección TCP/IP del nodo cliente existente la última vez que el nodo cliente contactó con el servidor. El campo se deja vacío si el software de cliente no admite la notificación de esta información al servidor.

ID exclusivo global



Identificador exclusivo global (GUID) utilizado la última vez que el nodo cliente estableció contacto con el servidor. Este GUID identifica el sistema principal donde está ubicado el nodo.

Archivos máximos en grupo de transacción

Especifica el número de archivos por validación de transacción que se transfieren entre un cliente y un servidor. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.



Ruta de grabación de datos

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento. Si no hay disponible una ruta, el nodo no puede enviar ningún dato.

 Sistemas operativos AIX  Sistemas operativos Linux Las opciones de la ruta de transferencia de datos son ANY, LAN o fuera de LAN.

Ruta de lectura de datos

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. Si no hay disponible una ruta, no es posible leer datos.

 Sistemas operativos AIX  Sistemas operativos Linux Las opciones de la ruta de transferencia de datos son ANY, LAN o fuera de LAN.

Iniciación de sesión

Controla si el servidor o el cliente ha de iniciar las sesiones. Están disponibles las dos opciones siguientes:

- ClientOrServer
- Serveronly

Dirección alto nivel

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados cuando SESSIONINITIATION se define con el valor SERVERONLY.

Dirección bajo nivel

Especifica el número de puerto del cliente en el que éste está a la escucha de las sesiones del servidor cuando SESSIONINITIATION se define con el valor SERVERONLY.

Nombre de grupo de proximidad

Especifica el nombre del grupo de proximidad al que pertenece un nodo. Si un nodo no pertenece a un grupo de proximidad, este campo está en blanco.

Consejo: Si el nodo contiene espacios de archivos que son miembros de un grupo de proximidad de espacio de archivos, este campo se deja en blanco. Puede encontrar nombres de espacio de archivos emitiendo el mandato QUERY FILESPACE.

Destino nodo proxy

Especifica qué nodos son nodos proxy (agentes) de otros nodos, en una lista separada por espacios. Si no hay ningún nodo en ese tipo de asociación, este campo está en blanco.

Agente de nodo proxy

Especifica el nombre de nodo originador (destino) para una sesión de nodo proxy en una lista separada por espacios. Si no hay ningún nodo en ese tipo de asociación, este campo está en blanco.

Grupos de nodos

Especifica el nombre del grupo de nodos al que pertenece un nodo. Si un nodo no pertenece a un grupo de nodos, este campo está en blanco.



Dirección de correo electrónico

Especifica la dirección de correo electrónico del nodo de cliente.

Eliminación de duplicados

La ubicación donde se eliminan los duplicados de los datos. El valor ServerOnly especifica que los duplicados de los datos almacenados en este nodo solo se pueden eliminar en el servidor. El valor Clientorserver especifica que los datos almacenados por este nodo se pueden deduplicar en el cliente o en el servidor.

Sistemas operativos AIX Sistemas operativos Linux Usuarios que pueden realizar copias de seguridad

 Sistemas operativos AIX  Sistemas operativos Linux Especifica si un ID de usuario no root o sólo un ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor. ALL indica que todos los usuarios pueden realizarla, mientras que ROOT indica que sólo el ID de usuario root puede realizar la copia de seguridad de los archivos en el servidor. Esta salida no está disponible si el sistema operativo del nodo cliente se considera un sistema operativo de usuario único.

Estado de réplica

Indica si el nodo está habilitado para la réplica. Son posibles los siguientes valores:

Habilitado

El nodo está configurado para la réplica y preparado para replicarse.

Inhabilitado

El nodo está configurado para la réplica pero no está preparado para replicarse.

Ninguno

El nodo no está configurado para la réplica.

Modalidad de réplica

Indica si el nodo está configurado como origen o destino de los datos replicados. Si este campo está en blanco, el nodo no está configurado para la réplica. Son posibles los siguientes valores:

Enviar

El nodo está configurado como origen de los datos para la réplica.

Recibir

El nodo está configurado como destino de los datos para la réplica.

SyncSend

Los datos que pertenecen al nodo van a estar sincronizados con los datos de nodo que hay en el servidor de réplica de destino. La sincronización se aplica sólo a los nodos cuyos datos se han importado desde un servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

SyncReceive

Los datos que pertenecen al nodo van a estar sincronizados con los datos de nodo que hay en el servidor de réplica de origen. La sincronización se aplica sólo a los nodos cuyos datos se han importado desde un servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

Ninguno

El nodo no está configurado para la réplica.

Servidor primario de réplica

Especifica el servidor de réplica de origen para el nodo de cliente.

Norma de réplica de copia de seguridad

Norma de réplica archivada

Norma de réplica de gestión de espacio

La regla de réplica que se aplica a los datos de copia de seguridad, archivados y gestionados por espacio que pertenecen al nodo. Son posibles los siguientes valores:

ALL_DATA

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL_DATA_HIGH_PRIORITY

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica `ACTIVE_DATA` excepto que los datos se replican con una prioridad alta.

DEFAULT

Replica los datos de copia de seguridad, archivado o gestionados por espacio según la regla de dominio para el tipo de datos.

NONE

No se replica ningún dato. Por ejemplo, si la regla de réplica de los datos de archivado es `NONE`, los datos de archivado que pertenecen al nodo no se replican.

Última duplicación en el servidor

Especifica el nombre del servidor al que se ha replicado por última vez el nodo y el nombre del servidor al que el cliente realiza la recuperación de errores durante las operaciones de restauración.

Nombre SO cliente

El sistema operativo del cliente. El asistente de despliegue del cliente utiliza esta información para desplegar un paquete en el cliente. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

Arquitectura de procesador de cliente

La arquitectura del cliente. El asistente de despliegue del cliente utiliza este valor para determinar qué paquete se desplegará cuando se esté actualizando el cliente. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

Productos cliente instalados

Los productos que se encuentran en el nodo. Se podrían listar los productos siguientes:

- BA (cliente de archivado y copia de seguridad)
- VE (entornos virtuales)
- FCM (FlashCopy Manager)

Versión de destino de cliente

La versión del cliente que se instalará en el momento planificado a través del mandato `DEFINE SCHEDULE` o `UPDATE SCHEDULE`. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

Autenticación

Especifica el método de autenticación de contraseña: `LOCAL`, `LDAP` o `LDAP` (pendiente).

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP
Este nodo está configurado para autenticarse con un servidor de directorio LDAP, pero el nodo aún no se autenticó.	LDAP (pendiente)

SSL necesario (en desuso)

Especifica si la configuración de seguridad para el nodo requiere capa de sockets seguros (SSL). Los valores pueden ser `SI`, `NO` o predeterminado. Debe tener autorización de nivel de sistema para actualizar el valor de nodo `SSLREQUIRED`. Este campo está en desuso.

Seguridad de sesión

Especifica el nivel de seguridad de sesión que se aplica para el nodo. Los valores pueden ser `STRICT` o `TRANSITIONAL`.

Método de transporte

Especifica el método de transporte que se ha utilizado la última vez para el nodo especificado. Los valores pueden ser `TLS 1.2`, `TLS 1.1` o `NONE`. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

Dividir objetos grandes

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. Sí indica que el servidor divide los objetos grandes (más de 10 GB) en fragmentos más pequeños cuando un nodo de cliente los almacena. No indica que este proceso se omite. El valor predeterminado es `Yes` (sí).

Tipo de riesgo

Especifica el tipo de evaluación de riesgo. Los valores pueden ser Predeterminado, Eludido o Personalizado. Predeterminado especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el mandato SET STATUSATRISKINTERVAL. Eludido especifica que el nodo no se evalúa para el estado de riesgo por el supervisor de estado. Personalizado indica que el nodo se evalúa con el intervalo que se ha especificado mediante el mandato SET NODEATRISKINTERVAL, en lugar del intervalo que se ha especificado mediante el mandato SET STATUSATRISKINTERVAL.

Intervalo de riesgo

Especifica el número de horas entre dos actividades de copia de seguridad del cliente, o dos actividades de réplica, después de lo cual el supervisor de estado indica que la actividad está en riesgo. Este campo contiene un valor únicamente cuando el campo Tipo en riesgo contiene el valor Personalizado.

URL de programa de utilidad

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde Centro de operaciones.

Recuperación de duplicación de archivos dañados

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino.

Fuera de servicio

Especifica si el nodo de cliente está fuera de servicio. Son posibles los siguientes valores:

YES

Especifica que el nodo está fuera de servicio.

Valor nulo

Especifica que el nodo no está fuera de servicio.

PENDING

Especifica que el nodo se está poniendo fuera de servicio o que el proceso para ponerlo fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso para poner fuera de servicio pendiente, siga las instrucciones de Poner fuera de servicio un nodo de cliente.

Fecha de fuera de servicio

Especifica la fecha en la que el nodo de cliente se quedó fuera de servicio.

Ejemplo: visualizar información acerca de los roles de nodo

La salida de ejemplo es sólo una porción de la pantalla completa.

```
query node alvin f=d
```

```
Agente de nodo proxy:
  Grupos de nodo:
    Dirección de correo electrónico:
    Optimización de almacenamiento: ServerOnly
  Usuarios permitidos para realizar copias de seguridad: Todos
  Rol: Servidor
  Alteración temporal de rol: UseReported
  Proveedor del procesador: ORACLE
  Marca del procesador: UltraSPARC-T2
  Tipo de procesador: 4
  Modelo de procesador:
  Número de procesadores: 1
  Hipervisor:
  Aplicación de la API: NO
  Error de exploración: NO
  Dirección MAC:
```

Descripciones de los campos

Rol

El rol de procesador que notifica el cliente.

Alteración temporal de rol

El valor de alteración temporal del rol, especificado con el mandato UPDATE NODE.

Proveedor de procesador

El proveedor de procesador que notifica el cliente.

Marca de procesador

La marca de procesador que notifica el cliente.

Tipo de procesador

El tipo de procesador que notifica el cliente. Este valor especifica el número de núcleos de procesador utilizados para el cálculo de PVU.

Modelo de procesador

- El modelo de procesador que notifica el cliente.
- Recuento de procesadores
 - El número de procesadores que notifica el cliente.
- Hypervisor
 - El hipervisor que notifica el cliente.
- Aplicación de API
 - El indicador del cliente que indica que el cliente es una aplicación de la API.
- Error de escaneo
 - El indicador de si la última exploración de información del procesador falla y necesita alguna investigación.
- Dirección MAC
 - La dirección MAC que notifica el cliente.

Ejemplo: ver todos los nodos que se autentican en el servidor de IBM Spectrum Protect

Si desea ver todos los nodos que se autentican localmente, especifique el mandato siguiente:

```
query node * authentication=local
```

Nombre nodo	Platafor.	Nombre dominio política	Días desde últ. acceso	Días desde contraseña	Bloqueado?
NODE1	WinNT	STANDARD	3	3	No
LOCAL	(?)	STANDARD	7	7	No

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY NODE

Mandato	Descripción
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.
RENAME NODE	Cambia el nombre de un nodo cliente.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

QUERY NODEDATA (Consultar datos de cliente en volúmenes)

Utilice este mandato para visualizar la información sobre los datos de uno o varios nodos de una agrupación de almacenamiento de acceso secuencial. QUERY NODEDATA visualiza el nombre del volumen en el que se escriben los datos de un nodo y la cantidad de espacio que ocupan los datos en dicho volumen. Esta información resulta útil al determinar la forma de agrupar nodos en agrupaciones de almacenamiento ubicadas próximas.

Clase de privilegio

Restricción: No puede utilizar este mandato para ver información de las agrupaciones de almacenamiento de contenedor.

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-|-----|
      v      |
>>-Query NODEData--+-+---nombre_nodo+-----+----->
      '-COLLOCGroup----grupo_proximidad-'
>-----+----->
      '-STGpool----nombre_agrupación-'
>-----+-----><
      '-VOLUME----nombre_vol-'

```

Parámetros

nombre_nodo

Especifica el nombre del nodo de cliente para el que desea localizar datos. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres. Debe especificar un nombre de nodo o un nombre de grupo de proximidad, pero no ambos.

COLLOCGroup

Especifica el nombre del grupo de proximidad para el que desea localizar datos. Debe especificar un nombre de nodo o un nombre de grupo de proximidad, pero no ambos.

Importante: Si la cantidad de espacio necesaria para completar la consulta sobre un grupo de proximidad supera el límite del almacenamiento intermedio SQL, el mandato QUERY NODEDATA puede fallar. Si el mandato falla por esta razón, emita el mandato QUERY COLLOCGROUP para visualizar una lista de los nodos del grupo. A continuación, emita el mandato QUERY NODEDATA para cada nodo del grupo.

STGpool

Especifica el nombre de la agrupación de almacenamiento secuencial que se va a consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar los nombres. Si un comodín coincide con el nombre de una agrupación de almacenamiento de disco, se pasará por alto el nombre de la agrupación de almacenamiento de disco. Si no especifica un valor para este parámetro, se consultarán todas las agrupaciones de almacenamiento secuenciales.

VOLUME

Especifica el volumen que contiene los datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar varios nombres. Si no especifica un valor para este parámetro, se consultarán todos los volúmenes de la agrupación de almacenamiento.

Utilizar comodines para visualizar datos de nodo para una agrupación de almacenamiento de acceso secuencial

Visualizar información sobre el lugar de almacenamiento de los datos de nodo de una agrupación de almacenamiento secuencial. Utilice un carácter de comodín para indicar los nombres de nodo. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodedata e*
```

Nombre	Nombre volumen	Nombre agrupación	Espacio físico almacen. ocupado (MB)
EDU_J2	E:\tsm\server\00000117.BFS	EDU512	0,01
EDU_J2	E:\tsm\server\00000122.BFS	EDU319	0,01
EDU_J3	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_J3	E:\tsm\server\00000120.BFS	EDU319	0,01

EDU_J7	E:\tsm\server\00000118.BFS	EDU512	0,04
EDU_J7	E:\tsm\server\00000123.BFS	EDU319	0,04
EDU_JJ1	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_JJ1	E:\tsm\server\00000121.BFS	EDU512	0,01

Visualizar información de datos de nodo para un grupo de proximidad específico

Visualizar la información sobre la ubicación de los datos de nodo de una agrupación de almacenamiento secuencial de un grupo de proximidad determinado. En este ejemplo, los nodos EDU_J3 y EDU_JJ1 son los únicos miembros que pertenecen al grupo de proximidad, grp1, e incluyen datos en una agrupación de almacenamiento de acceso secuencial.

```
query nodedata colloggroup=grp1
```

Nombre	Nombre volumen	Nombre agrupación	Espacio físico almacen. ocupado (MB)
-----	-----	-----	-----
EDU_J3	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_J3	E:\tsm\server\00000120.BFS	EDU319	0,01
EDU_JJ1	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_JJ1	E:\tsm\server\00000121.BFS	EDU512	0,01

Si especifica un grupo de proximidad de espacio de archivos, solo se visualizarán los volúmenes de los espacios de archivos pertenecientes al grupo de proximidad. Si especifica un grupo de proximidad de espacio de archivos y un volumen, se visualizarán los volúmenes del espacio de archivos dentro del grupo de proximidad que estén también en el volumen especificado.

Descripciones de los campos

Nombre del nodo

Especifica el nombre del nodo.

Nombre de volumen

Especifica el nombre del volumen que contiene los datos de nodo.

Nombre de la agrupación de almacenamiento

Especifica el nombre de la agrupación de almacenamiento a la que se asigna el volumen.

Espacio físico ocupado (MB)

Especifica la cantidad de espacio físico que ocupan los datos del nodo. El espacio físico incluye el espacio vacío dentro de los agregados, de donde pueden haberse suprimido o donde pueden haber caducado los archivos.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY NODEDATA

Mandato	Descripción
DEFINE COLLOGGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.

Mandato	Descripción
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

QUERY NODEGROUP (Consultar un grupo de nodos)

Utilice este mandato para visualizar los grupos de nodos definidos en el servidor.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-*-----
>>-Query NODEGroup--+-+-----+----->
      '-nombre_grupo-'

      .-Format----Standard----.
>-+-----+-----><
      '-Format----+Standard-+-'
      '-Detailed-'

```

Parámetros

nombre_grupo

Especifica el nombre del grupo de nodos que se visualizará. Para especificar varios nombres, utilice un carácter comodín. Este parámetro es opcional. El valor predeterminado es visualizar todos los grupos de nodos.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información. Para visualizar los miembros del grupo de nodos, debe especificar FORMAT=DETAILED.

Ejemplo: obtener una lista de los grupos de nodos del servidor

Visualizar los grupos de nodos definidos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodegroup
```

```

Nombre del grupo de nodos      Descripción del grupo de nodos
-----
DEPT_ED                       Departamento de formación
GROUP1                        Nodos cliente de baja capacidad.

```

Ejemplo: visualizar información detallada del grupo de nodos

Visualizar información completa sobre todos los grupos de nodos y determinar qué nodos cliente pertenecen a qué grupos de nodos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodegroup format=detailed
```

```

      Nombre del grupo de nodos: DEPT_ED
      Descripción del grupo de nodos: Departamento de formación
      Última actualización por (administrador): SERVER_CONSOLE
      Fecha/hora última actualización: 04/21/2006 10:59:03
      Miembro(s) del grupo de nodos: EDU_1 EDU_7

      Nombre del grupo de nodos: GROUP1

```

Descripción del grupo de nodos: nodos cliente de baja capacidad.
 Última actualización por (administrador): SERVER_CONSOLE
 Fecha/hora última actualización: 04/21/2006 10:59:16
 Miembro(s) del grupo de nodos: CHESTER REX NOAH JARED

Descripciones de los campos

Nombre de grupo de nodos
 El nombre del grupo de nodos.

Descripción de grupo de nodos
 La descripción del grupo de nodos.

Última actualización por (administrador)
 El nombre del administrador que ha definido o ha actualizado más recientemente el grupo de nodos.

Fecha/hora última actualización
 La fecha y hora en que el administrador ha definido o actualizado más recientemente el grupo de nodos.

Miembro(s) de grupos de nodos
 Los miembros del grupo de nodos.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY NODEGROUP

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)

Utilice este mandato para ver dónde están almacenados los espacios de archivos de cliente y cuánto espacio ocupan.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query OCCupancy----->
  .-*-----
>+-----+-----+----->
  |               .-*-----|
  |'-nombre_nodo--+'-----+'
  |               '-nombre_espacio_archivos-'
>+-----+-----+----->
  |'-STGpool-----'nombre_agrupación-'
```


El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen los nombres y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

CODEType

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre del espacio de archivos o cuando no especifique ningún nombre de espacio de archivos.

El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Los valores posibles son:

UNICODE

Incluir espacios de archivos que sólo están habilitados para Unicode.

NONUNICODE

Incluir espacios de archivos que no sólo están habilitados para Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

Ejemplo: visualizar los espacios de archivos asignados a un nodo específico

Visualizar información sobre dónde se almacenan todos los espacios de archivos asignados al nodo denominado DAISY. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query occupancy daisy
```

Nombre nodo	Tipo	Nombre espacio	FSID	Nombre agrup. almac.	Número de archivos	Espacio físico ocupado (MB)	Espacio lógico ocupado (MB)
DAISY	C.S.	DRIVED	1	COPYFILE	38	0,45	0,42

Ejemplo: visualizar los espacios de archivos asignados a un nodo específico que tienen un tipo de archivo de copia de seguridad

Visualizar información sobre los espacios de archivos que pertenecen al nodo WAYNE y que tienen un tipo de archivo de copia de seguridad. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query occupancy wayne type=backup
```

Nombre nodo	Tipo	Nombre espacio	FSID	Nombre agrup. almac.	Número de archivos	Espacio físico ocupado (MB)	Espacio lógico ocupado (MB)
WAYNE	C.S.	DWG1	1	BACKUPPOOL1	2.330	53,19	50,01
WAYNE	C.S.	OS2C	2	BACKUPPOOL1	1.554	32,00	31,30

Descripciones de los campos

Node Name

El nodo propietario del espacio de archivos. Si el nodo se ha suprimido anteriormente, se visualiza el nombre de nodo DELETED.

Type

El tipo de datos. Los valores posibles son:

Arch

Datos que se han archivado.

C.S.

Datos de los que se ha realizado una copia de seguridad.

G.E.

Datos que se han migrado desde un cliente IBM Spectrum Protect for Space Management.

Filespace Name

El nombre del espacio de archivos que pertenece al nodo.

Si el espacio de archivos se suprimió anteriormente, se visualiza el nombre de espacio de archivos DELETED.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre agrupación almacenamiento

La agrupación de almacenamiento donde está ubicado el espacio de archivos.

Número de archivos

El número de archivos lógicos que pertenecen al espacio de archivos y están almacenados en esta agrupación de almacenamiento. Al almacenar un archivo superior a 10 GB, el servidor divide el archivo en fragmentos de 10 GB. El número de fragmentos también está incluido en este valor para cálculos de ocupación.

Espacio físico ocupado (MB)

La cantidad de espacio físico ocupado por el espacio de archivos. El espacio físico incluye el espacio vacío dentro de los agregados, de donde pueden haberse suprimido o donde pueden haber caducado los archivos. Para este valor, 1 MB = 1048576 bytes.

Consejo: Este campo no visualiza un valor para las agrupaciones de almacenamiento que se han configurado para la eliminación de datos duplicados. Si desactiva la eliminación de datos duplicados para una agrupación de almacenamiento, no se visualizará ningún valor para la ocupación física hasta que no exista ningún archivo al que se haya aplicado la eliminación de duplicados en la agrupación de almacenamiento.

Espacio lógico ocupado (MB)

La cantidad de espacio ocupado por los archivos lógicos en el espacio de archivos. El espacio lógico es el espacio que se utiliza realmente para almacenar archivos, excluido el espacio vacío en los agregados. Para este valor, 1 MB = 1048576 bytes.

FSID

El identificador del espacio de archivos (FSID). El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY OCCUPANCY

Mandato	Descripción
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.

QUERY OPTION (Consultar opciones del servidor)

Utilice este mandato para visualizar la información sobre las opciones del servidor.

Cambie las opciones de servidor editando el archivo de opciones de servidor o bien emitiendo el mandato SETOPT. Cuando edita el archivo de opciones del servidor, debe volver a arrancar el servidor para que los cambios entren en vigor. Cualquier cambio que realice al emitir el mandato SETOPT entrará en vigor de forma inmediata.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query OPTion--+----->>
      .-*-----
      +-----+
      '-nombre_opción-'
```

Parámetros

nombre_opción

Especifica el nombre de una opción del archivo de opciones del servidor. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Se visualizarán todas las opciones del servidor que coincidan. Si no especifica este parámetro, se visualizará información acerca de todas las opciones.

Ejemplo: visualizar todas las opciones del servidor

Visualizar información acerca de todas las opciones del servidor. En la salida se indicarán todas las opciones y los valores que se han especificado para éstas.

```
query option
```

Ejemplo: visualizar los valores de las opciones empleando un carácter comodín

Ver los valores de todas las opciones que comienzan por L.

```
query option l*
```

Opción servidor	Valor opción
-----	-----
Language	AMENG

Ejemplo: visualizar los servidores de directorios LDAP

Ver los valores de todos los servidores de directorios LDAP.

```
query option ldapurl
```

Opción servidor	Valor opción
-----	-----
LDAP URL	ldap://tophoy.tucson.com\cn=tsmdata
LDAP URL	ldap://krypton.ibm.com\ou=tsmdata,dc=ibm,dc=com

Descripciones de los campos

Opción servidor

Especifica el nombre de la opción en el archivo de opciones de servidor.

Valor opción

Especifica el nombre de la opción en el archivo de opciones de servidor.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY OPTION

Mandato	Descripción
SETOPT	Actualiza una opción del servidor sin parar y reiniciar el servidor.

QUERY PATH (visualizar una definición de ruta)

Utilice este mandato para visualizar una ruta entre un origen y un destino.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

.-*-----
>>-Query PATH----->
| .-*-----|
|'-nombre_origen-----'|
|'-nombre_destino-'|

.-SRCType-----ANY-----
>+-----+----->
|'-SRCType-----+ANY-----+'
|+DATAMover+
|'-SERVer-----'|

.-DESTType-----ANY-----
>+-----+----->
|'-DESTType-----+ANY-----+'
|+DRIVE--LIBRary---library_name+
|'-LIBRary-----+'

.-Format-----Standard-----
>+-----+-----><
|'-Format-----+Standard-+-'
|'-Detailed-'|

```

Parámetros

nombre_origen

Especifica el nombre de un origen del que se visualizan las rutas. Este parámetro es opcional. Puede especificar caracteres comodín. El valor predeterminado es visualizar las rutas de todos los orígenes.

Un origen es un transportador de datos, un servidor o un agente de almacenamiento.

nombre_destino

Especifica el nombre de un destino del que se visualizan las rutas. Este parámetro es opcional. Puede especificar caracteres comodín. El valor predeterminado es visualizar las rutas de todos los destinos.

SRCType

Especifica el tipo de origen. Este parámetro es opcional. El valor predeterminado es visualizar las rutas de todos los tipos de origen. Los valores posibles son:

ANY

Especifica que se visualizarán las rutas con cualquier tipo de origen.

DATAMover

Especifica que sólo se visualizarán rutas con el tipo de origen DATAMOVER.

SERVer

Especifica que sólo se visualizarán rutas con el tipo de origen SERVER. (Un origen de tipo SERVER es un agente de almacenamiento.)

DESTType

Especifica el tipo de destino. Este parámetro es opcional. El valor predeterminado es visualizar las rutas de todos los tipos de destino. Los valores posibles son:

ANY

Especifica que se visualizarán las rutas con cualquier tipo de destino.

DRive

Especifica que sólo se visualizarán rutas con el tipo de destino DRIVE. Cuando el tipo de destino es una unidad, debe especificar el nombre de biblioteca. Puede especificar las rutas que deben visualizarse especificando un nombre en el parámetro LIBRARY.

LIBRary

Especifica que sólo se visualizarán las rutas cuyo tipo de destino sea LIBRARY.

LIBRary

Especifica el nombre de la biblioteca a la que pertenece la unidad. Este parámetro es necesario cuando el tipo de destino es una unidad (DESTTYPE=DRIVE).

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información de ruta de resumen

Visualizar información acerca de las rutas para el origen NETAPP1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path netapp1
```

Nombre orig	Tipo origen	Nombre destino	Tipo destino	Activado
NETAPP1	DATAMOVER	DRIVE1	DRIVE	Yes
NETAPP1	DATAMOVER	NASLIB	LIBRARY	Yes

Ejemplo: visualizar información de ruta detallada

Visualizar información detallada acerca de las rutas para el origen NETAPP1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path  
netapp1 format=detailed
```

 Sistemas operativos Linux

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: NASLIB  
Tipo destino: LIBRARY  
Biblioteca:  
Dispositivo: /dev/tmsmcsi/mc0  
Directorio:  
Activado: Yes  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora última actualización: 21/06/2002 20:52:56
```

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: DRIVE1  
Tipo destino: DRIVE  
Biblioteca: NASLIB  
Dispositivo: rst01  
Directorio:  
Activado: Yes  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora última actualización: 21/06/2002 20:55:23
```

 Sistemas operativos AIX  Sistemas operativos Windows

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: NASLIB  
Tipo destino: LIBRARY  
Biblioteca:  
Dispositivo: mc0  
Directorio:  
Activado: Yes  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora última actualización: 06/21/2001 20:52:56
```

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: DRIVE1  
Tipo destino: DRIVE  
Biblioteca: NASLIB  
Dispositivo: rst01  
Directorio:  
Activado: Yes  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora última actualización: 06/21/2001 20:55:23
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: mostrar información de ruta detallada de un servidor de medios de z/OS

Mostrar la información detallada sobre una ruta de servidor de medios de z/OS. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path format=detailed
```

```

Source Name: SERVER1
Tipo origen: SERVER
Nombre destino: ZOSMEDIA
Tipo destino: LIBRARY
Biblioteca:
Nombre nodo:
Dispositivo:
Gestor externo:
Servidor de medios ZOS: MEDSERV1
Método Método:
LUN:
Iniciador: 0
Directorio:
Activado: Yes
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 08/06/2011 15:33:39

```

Descripciones de los campos

Nombre de origen

El nombre del origen.

Nombre de destino

El nombre del destino.

Tipo de origen

El tipo del origen.

Tipo de destino

El tipo de destino.

Biblioteca

El nombre de la biblioteca que contiene la unidad de destino.

Este campo estará en blanco si el tipo de destino es una biblioteca. El nombre de biblioteca se encontrará en el campo de nombre de destino cuando el destino sea una biblioteca.

Node Name

El nombre del dispositivo que es el destino.

Dispositivo

El nombre del dispositivo que es el destino.

Gestor externo

El nombre del gestor externo.

Servidor de medios ZOS

El nombre del servidor de medios z/OS.

Método comunicaciones

Especifica el tipo de método de comunicación.

LUN

Especifica el nombre de unidad lógica mediante el cual el origen puede acceder al disco.

Iniciador

Especifica el iniciador de la comunicación.

Directorio

Especifica la ubicación de directorio de un archivo en el origen.

En línea

Especifica si la ruta está activada y disponible para utilizarla.

Última actualización por (administrador)

El ID del administrador que ha realizado la última actualización.

Fecha/hora de la última actualización

Fecha y hora en las que tuvo lugar la última actualización.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY PATH

Mandato	Descripción
DEFINE PATH	Define una ruta de un origen a un destino.

Mandato	Descripción
DELETE PATH	Suprime una ruta de un origen a un destino.
UPDATE PATH	Cambia los atributos asociados con una ruta.

QUERY POLICYSET (Consultar un juego de políticas)

Utilice este mandato para visualizar información sobre uno o varios juegos de políticas.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query Policyset----->
      .-*-----.
>+-----+----->
|          .-*-----|
|'-nom_dominio-+-----+'
|                   '-nombre_conjunto_políticas-'
|
|.-Format----Standard----.
>+-----+-----><
|'-Format----+Standard-+-'
|                   '-Detailed-'
```

Parámetros

nombre_dominio

Especifica el dominio de políticas asociado al juego de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los dominios de políticas. Debe especificar este parámetro cuando consulte un juego de políticas denominado explícitamente.

nombre_juego_políticas

Especifica el juego de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica ACTIVE o el nombre de un juego de políticas, se consultarán todos los juegos de políticas.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: obtener una lista de los juegos de políticas de todos los dominios

Consultar todos los juegos de políticas de todos los dominios de políticas. Crear la salida en formato estándar. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query policyset
```

Nombre dominio políticas	Nombre juego políticas	Nombre clase gestión archivos	Descripción del cliente
EMPLOYEE-RECORDS	ACTIVE	ACTIVEFI-LES	Dpto. de personal
EMPLOYEE-RECORDS	HOLIDAY	ACTIVEFI-LES	Dpto. de personal
EMPLOYEE-RECORDS	VACATION	ACTIVEFI-LES	Dpto. de personal
PROG1	SUMMER		Políticas grupo de programación

PROG2	SUMMER		Políticas grupo de programación
STANDARD	ACTIVE	STANDARD	Juego políticas predeterminado instalado.
STANDARD	STANDARD	STANDARD	Juego políticas predeterminado instalado.

Ejemplo: visualizar información detallada acerca de un juego de políticas específico

Consultar el juego de políticas VACATION que está en el dominio de políticas EMPLOYEE_RECORDS. Crear la salida en formato detallado. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query policyset employee_records vacation
format=detailed
```

```
Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre juego políticas: VACATION
Nombre clase gestión predeterminada: ACTIVEFILES
Descripción: Dpto. de personal
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/hora última actualización: 31/05/1998 13:15:50
Perfil gestión: ADSM_INFO
Cambios pendientes: Sí
```

Descripciones de los campos

Nombre de dominio de políticas

El nombre del dominio de políticas.

Nombre de juego de políticas

El nombre del juego de políticas.

Nombre clase gestión predeterminada

La clase de gestión asignada como la clase de gestión predeterminada para el juego de políticas.

Descripción

La descripción del juego de políticas.

Última actualización por (administrador)

El nombre del administrador o del servidor que ha actualizado por última vez el juego de políticas. Si este campo contiene \$\$CONFIG_MANAGER\$\$, el conjunto de políticas está asociado a un dominio que gestiona el gestor de configuración.

Fecha/hora última actualización

La fecha y la hora en que se ha definido o actualizado por última vez el juego de políticas.

Perfil de gestión

El perfil o los perfiles que gestionan el dominio al que pertenece este juego de políticas.

Cambios pendientes

Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

QUERY PROCESS (Consultar uno o más procesos de servidor)

Utilice este mandato para que se visualice información acerca de los procesos subordinados activos.

Para cancelar los procesos subordinados, emita el mandato CANCEL PROCESS. Para mostrar información detallada sobre los procesos de réplica de nodos, emita el mandato QUERY REPLICATION.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query PRocess--+-----+----->
                    '-process_number-'
>--+-----+--+-----+-----<
    '-DESCRiption-----serie-' '-STATus-----serie-'
```

Parámetros

número_proceso

Especifica el número de proceso subordinado que se ha de consultar. Este parámetro es opcional. Si no especifica, se visualizará información sobre todos los procesos subordinados.

DESCRiption

Especifica la serie de texto que desea buscar en la lista de descripciones de procesos activos. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

STATus

Especifica la serie de texto que desea buscar en la lista de estados de procesos activos. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

Ejemplo: consultar un único proceso subordinado

Visualizar información acerca del proceso en segundo plano 202. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process 202
```

Número proceso	Descripción proceso	Estado proceso
202	EXPORT SERVER	ANR0NNNI EXPORT Identificador MYEXPORTSERVER ANR0648I Se ha copiado lo siguiente: 8 dominios 2 juegos de políticas 10 Clases de gestión 4 Grupos de copia 1 administrador 746 Bytes (Se han detectado 0 errores) Volúmenes de entrada actuales: C:\BUILD\540\ GA\BUILD\NT\I386\DEBUG\ -00000014.BFS, (6 segundos)

Ejemplo: consultar todos los procesos subordinados

Visualizar información acerca de todos los procesos en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
proceso de consulta
```

Número proceso	Descripción proceso	Estado proceso
304	IDENTIFY DUPLICATES	Agrupación de almacenamiento FILEPOOL, Volumen /tsmpool2/00006664.

BFS, Archivos procesados:
 2000, Extensiones duplicadas
 encontradas: 344, Bytes duplicados
 encontrados: 3.238.123,
 Archivo físico actual
 (bytes): 2.626.676.296.
 Estado: Procesando

```

284 IDENTIFY
    DUPLICATES      Agrupación almacenamiento
                    FILEPOOL, Volumen
                    /tsmpool2/00006666.
                    BFS, Archivos procesados:
                    2000, Extensiones duplicadas
                    encontradas: 344, Bytes duplicados
                    encontrados: 3.238.123,
                    Archivo físico actual
                    (bytes): Ninguno.
                    Estado: En espera

4   Replicar nodo  Replicando nodo(s) IRONMAN.
                    Espacios de archivos completos: 0. Espacios
                    de archivos identificándose y
                    replicándose: 1. Espacios de archivos
                    replicándose: 0. Espacios de archivos
                    no iniciados: 3. Archivos actuales:
                    11.920. Archivos replicados: 0
                    de 0. Archivos actualizados: 0 de 0.
                    Archivos suprimidos: 0 de 0. Cantidad
                    replicada: 11.482 KB de 11.482
                    KB. Cantidad transferida: 11.482 KB.
                    Tiempo transcurrido: 0 día(s), 0 hora(s),
                    1 minutos(s).

37  Caducidad      Procesados 12 nodos de un total de
                    nodos, examinados 411 objetos,
                    suprimiendo 411 de copia de seguridad,
                    0 objetos de archivado,
                    0 volúmenes de copia de seguridad de BD,
                    0 archivos del plan de recuperación;
                    0 objetos reintentados y 0 errores
                    encontrados.
  
```

Ejemplo: consultar todos los procesos de réplica en segundo plano

Visualizar información acerca de todos los procesos de réplica en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process desc="replicate node"
```

Número proceso	Descripción proceso	Estado proceso
-----	-----	-----
4	Replicar nodo	Replicando nodo(s) IRONMAN. Espacios de archivos completos: 0. Espacios de archivos identificándose y replicándose: 1. Espacios de archivos replicándose: 0. Espacios de archivos no iniciados: 3. Archivos actuales: 11.920. Archivos replicados: 0 de 0. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 11.482 KB de 11.482 KB. Cantidad transferida: 11.482 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).

Ejemplo: consultar todos los procesos de réplica en segundo plano para un nodo específico

Visualizar información acerca de todos los procesos de réplica en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process desc="replicate node" status=ironman
```

Número proceso	Descripción proceso	Estado proceso
4	Replicar nodo	Replicando nodo(s) IRONMAN. Espacios de archivos completos: 0. Espacios de archivos identificándose y replicándose: 1. Espacios de archivos replicándose: 0. Espacios de archivos no iniciados: 3. Archivos actuales: 11.920. Archivos replicados: 0 de 0. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 11.482 KB de 11.482 KB. Cantidad transferida: 11.482 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).

Ejemplo: Verificar que se ha iniciado un proceso de recuperación de réplica

Después de iniciar un proceso de réplica de nodo con la recuperación de archivos habilitada, verifique que el servidor de réplica de destino ha iniciado el proceso de recuperación de archivo. Emita el mandato QUERY PROCESS en el servidor de réplica de destino. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Proceso proceso	Descripción proceso	Estado proceso
4	Replicar nodo - Recuperación.	Replicando nodo(s) 3MAUTOIMPORT. Espacios de archivos completos: 87. Espacios de archivos identificándose y replicándose: 0. Espacios de archivos replicando: 6. Espacios de archivos iniciados: 0. Archivos actuales: 0. Archivos replicados: 0 de 14. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 0 KB de 11.688 bytes. Cantidad transferida: 0 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minuto(s).

Ejemplo: Verificar que se recuperan los archivos dañados durante un proceso de réplica

Después de iniciar un proceso de réplica de nodo con la recuperación de archivos habilitada, verifique que los archivos dañados se están recuperando. Emita el mandato QUERY PROCESS en el servidor de réplica de origen. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Proceso proceso	Descripción proceso	Estado proceso
6	Replicar nodo (Como recuperación secundaria)	Recuperando archivos dañados del servidor SERVER2, proceso 4, número de sesiones activas 10.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: verificar que los archivos se convierten




Después de iniciar un proceso de conversión de agrupación de almacenamiento, verifique que los archivos se convierten. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Número proceso	Descripción proceso	Estado proceso
6	Convert Stgpool	Convirtiendo agrupación de almacenamiento FILEPOOL1 en una agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Volúmenes convertidos: 1 de 6, Volúmenes erróneos: 0, Archivos convertidos: 975, Bytes

convertidos: 196.27 MB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 151,27 MB

- 7 Convert Stgpool Convirtiendo agrupación de almacenamiento DEDUPPOOL en agrupación de almacenamiento de contenedores de directorio DIRPOOL. Archivos convertidos: 150 de 360, Bytes convertidos: 79.598 KB de 388 MB. Archivos no convertidos: 12. Bytes no convertidos: 27 MB. Volumen de entrada actual: /fvt/srv/BK01. Tiempo transcurrido: 0 Day(s), 0 hora(s), 1 minuto(s).
- 8 Convert Stgpool Convirtiendo agrupación de almacenamiento FILEPOOL1 en agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Archivos convertidos: 0, Bytes convertidos: 0 B de 1,00 GB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 0 B, Volumen de entrada actual: /STORAGE/file1/00000005.BFS, Tiempo transcurrido: 0 días, 0 horas, 1 minuto.
- 10 Convert Stgpool Convirtiendo agrupación de almacenamiento FILEPOOL1 en agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Archivos convertido: 1007, Bytes convertidos: 285.44 MB of 1.33 GB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 196.28 MB, Volumen de entrada actual: /STORAGE/file1/00000004.BFS, Tiempo transcurrido: 0 días, 0 horas, 1 minuto.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: Verificar el movimiento del disco local a la nube

Una vez iniciada la operación de transferencia de datos del disco local a la nube, verifique que los datos se están transfiriendo. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Número proceso	Descripción proceso	Estado proceso
4	Transfer local a nube	Transferencia de disco local a nube para la agrupación de almacenamiento de contenedores de directorio CLOUDPOOL. 1 contenedor procesado. 2.100 KB en 4 extensiones de datos transferidos. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).

Descripciones de los campos

Número de proceso

Especifica el número que se asigna al proceso en segundo plano activo.

Descripción de proceso

Especifica una descripción del proceso subordinado activo.

Estado de proceso

Especifica el estado del proceso subordinado activo.

Consejo: Cuando un proceso de réplica de nodo ha finalizado en el servidor de réplica de destino, sólo se almacena el proceso final en el servidor de réplica de destino, sólo la información de proceso final se almacena en la tabla de resumen de actividades. El resumen completo para el proceso de réplica se almacena en la tabla de resumen de actividad en el servidor de réplica de origen.

Mandatos relacionados

Tabla 1. Mandato relacionado con QUERY PROCESS

Mandato	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará información detallada.

USELocal

Al realizar la consulta desde un servidor gestionado, este parámetro especifica si la información del perfil se obtiene del gestor de configuración o del servidor gestionado. Si la información del perfil no existe en el servidor gestionado, la información se obtiene del gestor de configuración, independientemente del valor de este parámetro.

Si utiliza este parámetro en un servidor que no gestiona el gestor de configuración propietario del perfil, se hace caso omiso del parámetro. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la información del perfil, si está disponible, se obtiene del servidor gestionado. Si no hay información disponible del servidor gestionado, se establece contacto con el gestor de configuración.

No

Especifica que la información del perfil se obtiene del gestor de configuración aunque haya información disponible del servidor gestionado. De este modo se garantiza que recibirá información actual sobre el perfil.

Ejemplo: obtener una lista de perfiles de un gestor de configuración.

Visualizar la información de perfil de un gestor de configuración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query profile
```

Gestor configuración	Nombre perfil	Bloqueo
SERVER1	DEFAULT_PROFILE	No
SERVER1	ADMIN_INFO	No
SERVER1	EMPLOYEE	No
SERVER1	PERSONNEL	Yes

Ejemplo: visualizar información detallada de perfil para un servidor gestionado

Desde un servidor gestionado, visualizar información detallada actual para el perfil ADMIN_INFO. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Nota: Si el perfil está bloqueado, la mayoría de los campos no se visualizan.

```
query profile admin_info  
format=detailed uselocal=no
```

```
Gestor configuración: SERVER1  
Nombre perfil: ADMIN_INFO  
Bloqueo: No  
Descripción: Planificaciones de  
administración  
distribuidas  
Administradores de servidor: DENNIS EMILY ANDREA  
Dominios políticas: ADMIN RECORDS  
Planificaciones mandatos administración: ** todos los objetos **  
Scripts mandatos servidor:  
Conjuntos opciones cliente:  
Servidores:  
Grupos servidores:
```

Descripciones de los campos

Gestor de configuración

El nombre del gestor de configuración propietario del perfil.

Nombre de perfil

El nombre del perfil.

Bloqueo

Si el perfil está bloqueado.

Descripción

La descripción del perfil.

Administradores de servidor

- Los administradores que están asociados al perfil.
- Dominios de políticas
 - Los dominios de políticas que están asociados al perfil.
- Planificaciones de mandatos de administración
 - Las planificaciones de administración que están asociadas al perfil.
- Scripts de mandatos del servidor
 - Los scripts de mandatos que están asociados al perfil.
- Conjuntos de opciones de cliente
 - Los conjuntos de opciones de cliente que están asociados al perfil.
- Servidores
 - Los servidores que están asociados al perfil.
- Grupos de servidores
 - Los nombres de los grupos de servidores que están asociados al perfil.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

QUERY PROTECTSTATUS (Consultar estado de protección de una agrupación de almacenamiento)

Utilice este mandato para mostrar información sobre el estado de protección de las agrupación de almacenamiento de contenedores de directorio.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query PROTECTStatus-+-----+----->
                          .-*-----*
                          '-nombre_agrupación-'

.-Format----Standard----.
>+-----+-----><
  '-Format----+Standard+-'
    '-Detailed-'

```

Parámetros

nombre_agrupación

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que se va a consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor, se mostrará el estado de todas las agrupaciones de almacenamiento de contenedores de directorio.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: Visualización de información de resumen de una agrupación de almacenamiento específica

Visualizar información para una agrupación de almacenamiento denominada POOL1. Emita el mandato siguiente:

```
query protectstatus pool1
```

Source Server Name	Source Storage Pool	Target Server Name	Target Storage Pool	Pct. Protected	Last Complete Protect
NEXT	POOL1	NEXT	POOL1COPY	96.55	02/17/2017 11:15:07
NEXT	POOL1	NEXT1	POOL2	99.99	02/17/2017 11:14:53
NEXT	POOL1	UNKNOWN	UNKNOWN	UNKNOWN	02/17/2017 11:13:44
NEXT1	POOL2	NEXT	POOL1	100.00	02/17/2017 12:56:58

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Ejemplo: Visualización de información detallada de una agrupación de almacenamiento específica

Visualizar información detallada acerca de la agrupación de almacenamiento denominada EZLIFE. Emita el mandato siguiente:

```
query protectstatus pool1 format=detailed
```

```
Source Server Name: NEXT
Source Storage Pool: POOL1
Target Server Name: NEXT
Target Storage Pool: POOL1COPY
Porcentaje de Protected: 96.55
Data Extents Protected: 1,747
Data Extents Total: 1,852
Protected (MB): 165.33
Total (MB): 171.23
Last Completed Protection: 02/17/2017 11:15:07
Last Refresh Date/Time: 02/19/2017 00:27:12
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Descripciones de los campos

Source Server Name

El nombre del servidor de origen.

Agrupación de almacenamiento de origen

El nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen.

Target Server Name

El nombre del servidor de destino.

Agrupación de almacenamiento de destino

El nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de destino.

Porcentaje de Protegido

El porcentaje de datos protegidos en la agrupación de almacenamiento de contenedores de directorio.

Data Extents Protected

Número de extensiones de datos de la agrupación de almacenamiento de contenedores de directorio protegidas.

Data Extents Total

Número total de extensiones de datos en la agrupación de almacenamiento de contenedores de directorio.

Protected (MB)

Cantidad total de datos protegidos que se encuentran en la agrupación de almacenamiento de contenedores de directorio, en megabytes.

Total (MB)

Cantidad total de datos que se encuentran en la agrupación de almacenamiento de contenedores de directorio, en megabytes.

Last Completed Protection

La fecha y la hora de la última protección de la agrupación de almacenamiento de contenedores de directorio.

Last Refresh Date/Time

La fecha y la hora de la última actualización de la agrupación de almacenamiento de contenedores de directorio.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY PROTECTSTATUS

Mandato	Descripción
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.

QUERY PROXYNODE (Consulta la autorización de proxy de un nodo cliente)

Utilice este mandato para visualizar los nodos cliente que tienen autorización para actuar como proxy con otros nodos cliente del servidor de IBM Spectrum Protect.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query PROXynode---TArget-----.*-----  
+-----+-----+-----><  
'-nombre_nodo_destino-'
```

Parámetros

TArget

Especifica el nombre del nodo señalado por el nodo con autoridad proxy. Opcionalmente, se puede especificar un nombre de nodo de destino. Pueden utilizarse nombres comodín para especificar el nombre de nodo de destino. También se permite una lista separada por comas de nombres de nodo.

Ejemplo: obtener una lista de los nodos cliente que disponen de autorización de proxy

Para que se visualicen todos los nodos cliente de IBM Spectrum Protect que disponen de autorización de proxy para el nodo de destino denominado MYCLUSTER, emita el mandato siguiente.

```
query proxynode target=mycluster
```

```
Nodo destino      Nodo agente  
-----  
FRED              MOE MINIE MICKEY  
ALPHA            BETA GAMMA DELTA
```

Descripciones de los campos

Nodo destino

Especifica el nombre del nodo señalado por el nodo con autoridad proxy.

Nodo agente

Especifica el nombre del nodo de agente.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY PROXYNODE

Mandato	Descripción
---------	-------------

Mandato	Descripción
GRANT PROXYNODE	Concede autorización de proxy a un nodo agente.
REVOKE PROXYNODE	Revocar la autoridad de proxy a un nodo de agente.

QUERY PVUESTIMATE (Mostrar la estimación de unidades de valor de procesador)

Utilice este mandato para obtener una estimación de los dispositivos de cliente y los dispositivos de servidor que gestiona este servidor de IBM Spectrum Protect. Asimismo, este mandato proporciona una estimación de los totales de unidades de valor de procesador (PVU) para los dispositivos de servidor.

Este mandato genera una estimación de PVU basada en el número de nodos lógicos que hay definidos en el servidor de IBM Spectrum Protect. En cambio, el cálculo de obligaciones de licencia se basa en el número de sistemas físicos. Es posible que no exista una correlación unívoca entre el número de nodos lógicos y el número de sistemas físicos. El informe que genera el mandato QUERY PVUESTIMATE es una estimación, que no es vinculante jurídicamente.

Para el mandato QUERY PVUESTIMATE, los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de cliente. Los nodos en las demás plataformas se consideran dispositivos de servidor. El servidor en el que se ejecuta IBM Spectrum Protect también se clasifica como un dispositivo de servidor. No obstante, puede volver a clasificar los dispositivos de servidor como dispositivos de cliente si es necesario. Si el sistema incluye estaciones de trabajo retiradas, estaciones de trabajo de prueba u otras que puedan ignorarse a efectos de cálculo de PVU, especifíquelas como el tipo Otros. Para cambiar una clasificación de nodo, utilice el mandato UPDATE NODE o el mandato REGISTER NODE.

Nota: La información de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query PVUESTIMATE--+-Format-----Standard-----+<<
                          '-Format-----+-Standard+-'
                          '-Detailed-'

```

Parámetros

Format

Especifica el formato de salida. Este parámetro es opcional. El valor predeterminado es Standard. Se pueden utilizar los siguientes valores:

Standard

Especifica la salida estándar.

Detailed

Especifica la salida detallada.

Ejemplo: visualizar el número estimado de dispositivos y PVU

Visualice el número estimado de dispositivos de cliente y dispositivos de servidor, y la PVU estimada de los dispositivos de servidor para un servidor de IBM Spectrum Protect. Emita el mandato siguiente:

```
query pvueestimate
```

Tabla 1. Salida de ejemplo de varios productos gestionados por un servidor de IBM Spectrum Protect

Producto	Número de dispositivos de cliente	Número de dispositivos de servidor	PVU de dispositivos de servidor
IBM Spectrum Protect Extended Edition	1.000	905	90.500

Producto	Número de dispositivos de cliente	Número de dispositivos de servidor	PVU de dispositivos de servidor
IBM Spectrum Protect para redes de área de almacenamiento	50	10	1.000
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect para correo	0	25	5.000
IBM Spectrum Protect para bases de datos	0	1.025	20.500
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
IBM Spectrum Protect para recuperación y copia de seguridad del sistema	0	0	0
Otras clasificaciones de nodos	Número		
Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente	10		
Nodos de la versión 6.3 o posteriores sin coincidencia de PVU	9		
Nodos clasificados por el administrador como "otros dispositivos"	8		
Nodos definidos como una aplicación de API sin licencia	6		

La lista siguiente incluye detalles sobre los campos de ejemplo:

Producto

El nombre de producto IBM Spectrum Protect.

Número de dispositivos de cliente

El número estimado de dispositivos de cliente que gestiona el producto. De forma predeterminada, solo los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de cliente.

Número de dispositivos de servidor

El número estimado de dispositivos de servidor que gestiona el producto. De forma predeterminada, solo los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de servidor. Este número también incluye el servidor en el que se ejecuta IBM Spectrum Protect.

PVU de dispositivos de servidor

Las PVU estimadas de todos los nodos que están conectados como dispositivos de servidor.

Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente

Los dispositivos que no notifican información de procesador al servidor.

Nodos de la versión 6.3 o posteriores sin coincidencia de PVU

Dispositivos que no notifican todos los valores necesarios o que notifican algunos valores como "Desconocido".

Nodos clasificados por el administrador como "otros dispositivos"

Los nodos que el administrador excluye del recuento de PVU utilizando el mandato update node roleoverride=other.

Nodos definidos como una aplicación de API sin licencia

Nodos como, por ejemplo, las aplicaciones de API personalizadas o de copia de seguridad de DB2.

Ejemplo: visualizar información detallada del nodo

Visualice información de nodos individuales especificando el valor detallado (d) para el parámetro Format. Emita el mandato siguiente:

```
tsm: PATMOS_630> query pvuestimate f=d
```

Tabla 2. Clasificaciones de nodos para productos específicos

Producto	Número de dispositivos de cliente	Número de dispositivos de servidor	PVU de dispositivos de servidor
IBM Spectrum Protect Extended Edition	1.000	905	90.500
- banode1	1		
- banode2		1	200
- banode3	1		
- banode3		1	100
IBM Spectrum Protect para redes de área de almacenamiento	50	10	1.000

Producto	Número de dispo. de cliente	Número de dispo. de servidor	PVU de dispo. de servidor
- stagent1		1	50
- stagent2		1	100
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect para correo	0	25	5.000
- mailnode1		1	200
- mailnode2		1	100
IBM Spectrum Protect para bases de datos	0	1.025	20.500
- dbnode1		1	200
- dbnode2		1	100
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
- erpnode1		1	50
- erpnode2		1	100
IBM Spectrum Protect para recuperación y copia de seguridad del sistema	0	0	0
Otras clasificaciones de nodos	Número		
Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente	10		
- oldnode1	1		
- oldnode2	1		
- mailnote44	1		
- erpnode66	1		
Nodos de la versión 6.3 o posteriores sin coincidencia de PVU	10		
- badcitnode1	1		
- badcitnode2	1		
- mailnode23	1		
- erpnode34	1		
Nodos clasificados por el administrador como "otros dispositivos"	8		
- overriddennode1	1		
- overriddennode2	1		
- mailnode77			
Nodos definidos como una aplicación de API sin licencia	6		
- vendorapinode1	1		
- vendorapinode2	1		

Mandatos relacionados

Tabla 3. Mandatos relacionados con QUERY PVUESTIMATE

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

QUERY RECOVERYMEDIA (Consultar medio de recuperación)

Utilice este mandato para visualizar información sobre el medio (por ejemplo, medio de arranque) necesario para efectuar la recuperación de una máquina. Los medios se visualizan por orden alfabético de nombres.

Recuerde: IBM Spectrum Protect no utiliza la información. Sólo está disponible para ayudar a planificar la recuperación ante siniestro de las máquinas cliente.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query RECOVERYMedia-+-----+----->
                          .-*-----+
                          '-nombre_medio-'

>+-----+-----+-----+----->
  '-Type-----+B0ot--+-'  '-L0cation-----ubicación-'
                          '-OTher-'

  .-Format-----Standard-----
>+-----+-----+-----+-----><
  '-Format-----+Standard--+-'
                          '-Detailed-'
  
```

Parámetros

nombre_medio

Especifica el nombre del medio de recuperación. Puede utilizar caracteres comodín para especificar el nombre. Este parámetro es opcional. El valor predeterminado son todos los medios de recuperación.

Type

Especifica el tipo de medios que se han de consultar. Este parámetro es opcional. Si no se especifica este parámetro, se consultarán todos los medios de recuperación. Los valores posibles son:

B0ot

Sólo se consultan los medios de arranque.

OTher

Se consultan todos los medios excepto los de arranque.

L0cation

Especifica la ubicación del medio de recuperación que se ha de consultar. Este parámetro es opcional. Puede especificar hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. Los valores posibles son:

Standard

Visualiza información parcial. Este es el valor predeterminado.

Detailed

Visualiza toda la información.

Ejemplo: visualizar información de resumen acerca de medios de recuperación específicos

Visualizar información para el medio de recuperación denominado RECMED1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query recoverymedia RECMED1
```

Nombre medio recuperación	Nombres volúmenes	Ubicación	Nombre máquina
RECMED1	vol1 vol2 vol3 vol4	IRONMOUNTAIN	MACH1

Ejemplo: visualizar información detallada acerca de medios de recuperación específicos

Visualizar información detallada acerca del medio de recuperación denominado RECMED1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query recoverymedia RECMED1 format=detailed
```

```
Nombre medio recuperación: RECMED1
Tipo: Arranque
Nombres volúmenes: vol1 vol2 vol3 vol4
Ubicación: IRONMOUNTAIN
Descripción:
Producto:
Información producto:
Nombre máquina: MACH1
```

Descripciones de los campos

Nombre del medio de recuperación

El nombre del medio de recuperación.

Tipo

Si el medio de recuperación es de tipo arranque o de otro tipo. Los valores posibles son:

Arranque

El medio de recuperación es de tipo arranque.

Otro

El medio de recuperación no es de tipo arranque.

Nombres de volúmenes

Especifica el conjunto de volúmenes que contiene los datos necesarios para efectuar la recuperación para las máquinas asociadas a este medio.

Ubicación

Lugar donde se almacena el medio de recuperación.

Descripción

La descripción del medio de recuperación.

Producto

El producto utilizado para crear el medio de arranque.

Información de producto

Información acerca del producto que ha creado el medio de arranque. Es posible que esta información sea necesaria para restaurar la máquina.

Nombre de máquina

Las máquinas que están asociadas a este medio de recuperación.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY RECOVERYMEDIA

Mandato	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

QUERY REPLICATION (Consultar los procesos de réplica de nodos)

Utilice este mandato para visualizar la información sobre la ejecución y la finalización de procesos de réplica de nodos.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Importante: No puede visualizar información sobre la ejecución de los procesos de réplica para los nodos cliente que se están convirtiendo de operaciones de importación y exportación a operaciones de réplica. El proceso de conversión podría ejecutarse durante un largo periodo de tiempo, pero sólo se produce una vez para un nodo cliente que se está convirtiendo.

De forma predeterminada, los registros sobre los procesos de réplica de nodos completados se retienen durante 30 días naturales. Un *día natural* consta de 24 horas, de medianoche a mediodía.

Para visualizar el periodo de retención, emita el mandato QUERY STATUS. Compruebe el valor en el campo Período de retención de registros de réplica. Para cambiar el periodo de retención, emita el mandato SET REPLRETENTION.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query REPLIcation--nombre_nodo----->
. -*----- .
>----->
| (1) |
|-----+---nombre_espacio_archivos---+---|
| |-----+---FSID---+---|
| | (2) |
| |-----+---|
. -NAMEType----SERVER----- .
>----->
| -NAMEType----+---SERVER---+---|
| |-----+---UNICODE---+---|
| | (2) |
| |-----+---FSID-----|
. -CODEType----BOTH----- .
>----->
| -CODEType----+---BOTH-----+---|
| |-----+---UNICODE-----+---|
| |-----+---NONUNICODE---|
. -DISplay----1----- .
>----->
| -DISplay----+---número_de_días---|
. -PROcessid----identificador_proceso-|
. -STATUS----ALL----- . -Format----Standard----- .
>----->
| -STATUS----+---ALL-----+---| -Format----+---Standard+-| | |
| |-----+---RUNNING---+---| |-----+---Detailed-|
| |-----+---ENDED---+---|
| |-----+---FAILED---|
```

Notas:

1. No mezcle los FSID (identificadores de espacio de archivos) y los nombres de espacio de archivos en el mismo mandato.
2. No especifique un FSID si utiliza caracteres comodín para el nombre del nodo de cliente.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se ha de consultar. Puede utilizar caracteres comodín cuando especifique este nombre, con una excepción. Si el valor del parámetro NAMETYPE es FSID, no especifique caracteres comodín para el nombre del nodo de cliente. El valor FSID indica el identificador del espacio de archivos. Los espacios de archivos con nombres idénticos pueden identificadores diferentes en nodos de cliente diferentes.

nombre_espacio_archivos o FSID

Especifica el nombre del espacio de archivos o el identificador del espacio de archivos (FSID) que se ha de consultar. Un nombre o FSID es opcional. Si no especifica un nombre o un FSID, se consultan todos los espacios de archivos.

nombre_espacio_de_archivos

Especifica el nombre del espacio de archivos que tiene los datos que se van a consultar. Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos, emita el mandato QUERY FILESPACE. Cuando existan varios nombres, separe éstos mediante comas, sin espacios intercalados. Cuando especifique el nombre, puede utilizar caracteres comodín.

Un servidor que tenga clientes con espacios de archivos activados para Unicode puede que deba convertir el nombre del espacio de archivos. Por ejemplo, puede que el servidor deba convertir un nombre de la página de códigos del servidor a Unicode. Para obtener información adicional, consulte el parámetro NAMETYPE. Si no especifica ningún nombre de espacio de archivos o especifica sólo un único carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

FSID

Especifica el identificador del espacio de archivos que se va a consultar. El servidor utiliza los FSID para encontrar los espacios de archivos que se deben replicar. Para determinar el FSID de un espacio de archivos, emita el mandato QUERY FILESPACE. Cuando existan varios FSID, sepárelos mediante comas, sin espacios intercalados. Si especifica un FSID, el valor del parámetro NAMETYPE debe ser FSID.

NAMEType

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y que tienen sistemas operativos de Windows, Macintosh OS X o NetWare.

Utilice este parámetro sólo si especifica un nombre de espacio de archivos parcial o totalmente completo. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor. La conversión también puede fallar si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacio de archivos utilizando los identificadores de espacios de archivos.

CODEType

Especifica el tipo de espacios de archivos que se van a incluir en la consulta. El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo si especifica un único carácter comodín para el nombre del espacio de archivos. Puede especificar uno de los siguientes valores:

UNICODE

Incluir solo espacios de archivos que están en Unicode.

NONUNICODE

Incluir únicamente espacios de archivos que no estén en Unicode.

BOTH

Incluir todos los espacios de archivos independientemente del tipo de página de códigos.

DISplay

Especifica el número de días de historial de réplicas de nodos que se muestran. El valor predeterminado es 1, que muestra información sobre la ejecución de procesos de réplica de nodo y sobre procesos que se han completado durante el día natural actual. El valor máximo es 9999.

Puede especificar un número que sea igual o menor que el número de días que se han especificado como periodo de retención para los registros de historial de réplicas. Si especifica un valor que es superior al valor del periodo de retención de réplica o superior al número de días en los que se recopilan registros de réplica, el servidor sólo muestra el número de registros de historial de réplica que están disponibles. Por ejemplo, suponga que el periodo de retención de réplica es 30 días y que el proceso de réplica se ejecuta sólo durante 10 días. Si especifica `DISPLAY=20`, sólo se visualizan 10 días del historial de réplica.

PROcessid

Especifica el historial de réplicas de nodos asociado con un determinado proceso identificado por el identificador de proceso. Este parámetro es opcional. Si no especifica este parámetro, se visualizarán todos los procesos para el número de días que especifica el parámetro `DISPLAY`.

El reinicio del servidor puede hacer que este reutilice los ID de proceso. La reutilización de ID de proceso puede generar ID de proceso duplicados para procesos diferentes.

STatus

Especifica el estado de los espacios de archivos a consultar. Este parámetro es opcional. El valor predeterminado es `ALL`. Puede especificar uno de los siguientes valores:

ALL

Especifica todos los espacios de archivos que se están replicando, espacios de archivos que se han replicado correctamente y espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

RUNning

Especifica todos los espacios de archivos que se están replicando en el servidor de réplica de destino.

ENded

Especifica todos los espacios de archivos que se han replicado correctamente y espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

FAiled

Especifica todos los espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es `STANDARD`. Puede especificar uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial sobre los procesos de réplica de nodos.

Detailed

Especifica que se visualizará toda la información disponible sobre los procesos de réplica de nodos.

Ejemplo: visualizar información sobre los procesos de réplica para un espacio de archivos

Visualice información sobre los procesos de réplica para un espacio de archivos en el nodo de cliente `PAYROLL`. El identificador del espacio de archivos es 10.

```
query replication ironman
```

NodeName	Nombre archivos	FSID	Hora de inicio del cliente	Hora de finalización	Estado	Fase
IRONMAN	/space	2	02/08/11 21:44:19	02/08/11 21:48:14	Finalizado	Ninguna

```
query replication ironman format=detailed
```

```
Nombre nodo: IRONMAN
Nombre de espacio de archivos: /space
FSID: 2
Hora de inicio: 02/08/11 21:44:19
Hora de finalización: 02/08/11 21:48:14
Estado: Finalizado
Número de proceso: 4
Mandato: replicate node ironman
Fase: Ninguna
```

```

Tiempo de ejecución de proceso: 0 día(s) 0 hora(s)
                                4 Minuto(s)
Estado de terminación: Completo
Razón de no completarse: Ninguna
Fecha/hora última actualización de copia de seguridad:
Servidor de destino de copia de seguridad:
Archivos de copia de seguridad que no necesitan ninguna acción: 0
  Archivos de copia de seguridad que se replican: 0
  Archivos de copia de seguridad replicados: 0
Archivos de copia de seguridad no replicados debido a errores: 0
  Archivos de copia de seguridad no replicados todavía: 0
  Archivos de copia de seguridad que se suprimen: 0
  Archivos de copia de seguridad suprimidos: 0
Archivos de copia de seguridad no suprimidos debido a errores: 0
  Archivos de copia de seguridad que se actualizan: 0
  Archivos de copia de seguridad actualizados: 0
Archivos de copia de seguridad no actualizados debido a errores: 0
  Bytes de copia de seguridad que se replican (MB): 0
  Bytes replicados de copia de seguridad (MB): 0
  Bytes transferidos de copia de seguridad (MB): 0
  Bytes de copia de seguridad no replicados
    debido a errores (MB): 0
  Bytes no replicados todavía de copia de seguridad (MB): 0

Fecha/hora última actualización de archivado: 02/08/11 21:48:14
Servidor de destino de archivado: NIGLINA
Archivos de archivado que no necesitan ninguna acción: 0
  Archivos de archivado que se replican: 39.416
  Archivos de archivado replicados: 39.206
Archivos de archivado no replicados debido a errores: 210
  Archivos de archivado no replicados todavía: 0
  Archivos de archivado que se suprimen: 0
  Archivos de archivado suprimidos: 0
Archivos de archivado no suprimidos debido a errores: 0
  Archivos de archivado que se actualizan: 0
  Archivos de archivado actualizados: 0

Archivos de archivado no actualizados debido a errores: 0
  Bytes de archivado que se replican (MB): 4.335
  Bytes replicados de archivado (MB): 4.335
  Bytes transferidos de archivado (MB): 0
  Bytes de archivado no replicados
    debido a errores (MB): 0
  Bytes no replicados todavía de archivado (MB): 0

Fecha/hora última actualización de gestionados por espacio:
Servidor destino de gestión de espacio:
Archivos gestionados por espacio que no necesitan ninguna acción: 0
  Archivos gestionados por espacio que se replican: 0
  Archivos gestionados por espacio replicados: 0
  Archivos gestionados por espacio no replicados
    debido a errores: 0
Archivos gestionados por espacio no replicados todavía: 0
  Archivos gestionados por espacio que se suprimen: 0
  Archivos gestionados por espacio suprimidos: 0
Archivos de archivado no suprimidos
  debido a errores: 0
  Archivos gestionados por espacio que se actualizan: 0
  Archivos gestionados por espacio actualizados: 0
Archivos gestionados por espacio no actualizados
  debido a errores: 0
  Bytes gestionados por espacio que se replican (MB): 0
  Bytes replicados gestionados por espacio (MB): 0
  Bytes transferidos gestionados por espacio (MB): 0
  Bytes gestionados por espacio no replicados
    debido a errores (MB): 0
  Bytes no replicados todavía gestionados por espacio (MB): 0
  Total de archivos que no necesitan ninguna acción: 0
  Total de archivos que se replican: 39.416
  Total de archivos replicados: 39.206
Total de archivos no replicados debido a errores: 210
  Total de archivos no replicados todavía: 0
  Total de archivos que se suprimen: 0
  Total de archivos suprimidos: 0
Total de archivos no suprimidos debido a errores: 0
  Total de archivos que se actualizan: 0

```

Total de archivos actualizados: 0
Total de archivos no actualizados debido a errores: 0
Total de bytes que se replican (MB): 4.335
Total de bytes replicados (MB): 4.335
Total de bytes transferidos (MB):
Total de Bytes no replicados
Debido a errores (MB):
Total de bytes no replicados todavía (MB):
Porcentaje de terminación estimado: 100
Tiempo estimado restante:
Hora estimada de terminación:

Descripciones de los campos

Nombre del nodo

El nombre del nodo de cliente cuyos datos se están mostrando.

Nombre de espacio de archivos

El nombre del espacio de archivos de cliente cuyos datos se están mostrando.

FSID

El identificador del espacio de archivos.

Hora de inicio

La fecha y la hora en que se ha iniciado el proceso de réplica de nodo.

Hora de finalización

La fecha y la hora en que ha finalizado el proceso de réplica de nodo.

Estado

El estado del proceso de réplica de nodo. Son posibles los siguientes valores:

Ejecutando

El proceso está activo y está buscando datos seleccionables o enviando datos al servidor de réplica de destino.

Finalizado

El proceso ha finalizado o ha fallado.

No válido

El proceso ha fallado.

Número de proceso

El identificador del proceso de réplica de nodo.

El mismo número de proceso puede tener distintas horas de inicio. Si se inicia un proceso de réplica y se reinicia el servidor, el servidor empieza a asignar números de proceso que empiezan por el número 1. Los procesos de réplica que se inician después de un reinicio del servidor pueden obtener los números de proceso que ya se han asignado a otros procesos de réplica en el historial de réplicas. Para identificar procesos de réplica exclusivos, utilice la hora de inicio.

Mandato

El mandato que se ha emitido para iniciar el proceso de réplica de nodo.

Fase

La fase de un proceso de réplica de nodo en ejecución. Las siguientes fases se muestran en el orden en el que se producen:

Identificando

El proceso de réplica de nodo ha empezado a identificar los datos que se van a replicar, pero los datos no se están enviando todavía al servidor de réplica de destino.

Identificando y replicando

El proceso de réplica de nodo está identificando los datos que se van a replicar y transfiriendo los datos al servidor de réplica de destino.

Replicando

El proceso de réplica de nodo ha identificado los datos y transfiere los archivos al servidor de réplica de destino.

Ninguno

El proceso de réplica de nodo no se está ejecutando.

Tiempo de ejecución de proceso

El tiempo de ejecución del proceso de réplica de nodo.

Estado de finalización

El estado del proceso de réplica de nodo. Son posibles los siguientes valores:

Completo

El proceso de réplica de nodo se ha completado.

No completo

El proceso de réplica de nodo ha finalizado sin ejecutarse completamente. Para determinar la razón, compruebe el valor en el campo Razón de no completarse.

Razón de la no finalización

La razón por la que ha finalizado el proceso de réplica de nodo sin completarse. Los valores posibles incluyen *cancelled* y *other*. El valor *other* puede indicar que se ha parado el servidor durante la réplica o que el servidor ha fallado.

Fecha/hora última actualización de copia de seguridad

La fecha y la hora en que se han actualizado por última vez las estadísticas de copia de seguridad. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Fecha/hora última actualización de archivado

La fecha y la hora en que se han actualizado por última vez las estadísticas de archivado. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Fecha/hora de la última actualización de gestionados por espacio

La fecha y la hora en que se han actualizado por última vez las estadísticas de los archivos gestionados por espacio. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Servidor destino de copia de seguridad

El nombre del servidor de réplica de destino para los archivos de copia de seguridad.

Servidor destino de archivado

El nombre del servidor de réplica de destino para los archivos de archivado.

Servidor destino de gestión de espacio

El nombre del servidor de réplica de destino para los archivos gestionados por espacio.

Archivos de copia de seguridad que no necesitan acción

El número de archivos de copia de seguridad del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Copias archivadas que no necesitan acción

El número de archivos de archivado del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Archivos de espacio gestionado que no necesitan acción

El número de archivos gestionados por espacio del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Archivos de copia de seguridad para replicar

El número de archivos de copia de seguridad que deben replicarse en el servidor de réplica de destino.

Copias archivadas para replicar

El número de archivos de archivado que deben replicarse en el servidor de réplica de destino.

Archivos gestionados por espacio para replicar

El número de archivos gestionados por espacio que deben replicarse en el servidor de réplica de destino.

Archivos de copia de seguridad replicados

El número de archivos de copia de seguridad que se han replicado en el servidor de réplica de destino.

Archivos de archivado replicados

El número de archivos de archivado que se han replicado en el servidor de réplica de destino.

Archivos gestionados por espacio replicados

El número de archivos gestionados por espacio que se han replicado en el servidor de réplica de destino.

Archivos de copia de seguridad no replicados debido a errores

El número de archivos de copia de seguridad que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos de archivado no replicados debido a errores

El número de archivos de archivado que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no replicados debido a errores

El número de archivos gestionados por espacio que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos de copia de seguridad aún no replicados

El número de archivos de copia de seguridad que no se han replicado todavía en el servidor de réplica de destino.

Archivos de archivado aún no replicados

El número de archivos de archivado que no se han replicado todavía en el servidor de réplica de destino.

Archivos gestionados por espacio aún no replicados

El número de archivos gestionados por espacio que no se han replicado todavía en el servidor de réplica de destino.

Archivos de copia de seguridad para suprimir

El número de archivos de copia de seguridad que deben suprimirse en el servidor de réplica de destino.

Archivos de archivado para suprimir

El número de archivos de archivado que deben suprimirse en el servidor de réplica de destino.

Archivos gestionados por espacio para suprimir

El número de archivos gestionados por espacio que deben suprimirse en el servidor de réplica de destino.

Archivos de copia de seguridad suprimidos

El número de archivos de copia de seguridad que se han suprimido en el servidor de réplica de destino.

Archivos de archivado suprimidos

El número de archivos de archivado que se han suprimido en el servidor de réplica de destino.

Archivos gestionados por espacio suprimidos

El número de archivos gestionados por espacio que se han suprimido en el servidor de réplica de destino.

Archivos de copia de seguridad no suprimidos debido a errores

El número de archivos de copia de seguridad que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos de archivado no suprimidos debido a errores

El número de archivos de archivado que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no suprimidos debido a errores

El número de archivos gestionados por espacio que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos de copia de seguridad para actualizar

El número de archivos de copia de seguridad que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos de archivado para actualizar

El número de archivos de archivado que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos gestionados por espacio para actualizar

El número de archivos gestionados por espacio que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos de copia de seguridad actualizados

El número de archivos de copia de seguridad que se han actualizado en el servidor de réplica de destino.

Archivos de archivado actualizados

El número de archivos de archivado que se han actualizado en el servidor de réplica de destino.

Archivos gestionados por espacio actualizados

El número de archivos gestionados por espacio que se han actualizado en el servidor de réplica de destino.

Archivos de copia de seguridad no actualizados debido a errores

El número de archivos de copia de seguridad que no se han actualizado en el servidor de réplica de destino debido a errores.

Archivos de archivado no actualizados debido a errores

El número de archivos de archivado que no se han actualizado en el servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no actualizados debido a errores

El número de archivos gestionados por espacio que no se han actualizado en el servidor de réplica de destino debido a errores.

Bytes de copias de seguridad para replicar (MB)

El número de bytes de copia de seguridad que deben replicarse en el servidor de réplica de destino.

Bytes de archivado para replicar (MB)

El número de bytes de archivado que deben replicarse en el servidor de réplica de destino.

Bytes gestionados por espacio para replicar (MB)

El número de bytes gestionados por espacio que deben replicarse en el servidor de réplica de destino.

Bytes de copias de seguridad replicados (MB)

El número de bytes de copia de seguridad que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes de archivados replicados (MB)

El número de bytes de archivado que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes gestionados por espacio replicados (MB)

El número de bytes gestionados por espacio que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes de copias de seguridad transferidos (MB)

El número de bytes de copia de seguridad que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes de archivados transferidos (MB)

El número de bytes de archivado que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes gestionados por espacio transferidos (MB)

El número de bytes gestionados por espacio que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes de copia de seguridad no replicados debido a errores (MB)

El número de bytes de copia de seguridad que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes de archivado no replicados debido a errores (MB)

El número de bytes de archivado que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes gestionados por espacio no replicados debido a errores (MB)

El número de bytes gestionados por espacio que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes de copia de seguridad aún no replicados (MB)

El número de bytes de copia de seguridad que aún no se han replicado en el servidor de réplica de destino.

Bytes de archivados aún no replicados (MB)

El número de bytes de archivado que aún no se han replicado en el servidor de réplica de destino.

Bytes gestionados por espacio aún no replicados (MB)

El número de bytes gestionados por espacio que aún no se han replicado en el servidor de réplica de destino.

Total de archivos que no necesitan acción

El número total de archivos en el espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Total de archivos para replicar

El número total de archivos que se replican en el servidor de réplica de destino.

Total de archivos replicados

El número total de archivos que se han replicado en el servidor de réplica de destino.

Total de archivos no replicados debido a errores

El número total de archivos que no se han replicado debido a errores.

Total de archivos no replicados todavía

El número total de archivos que no se han replicado todavía en el servidor de réplica de destino.

Total de archivos para suprimir

El número total de archivos que se han suprimido en el servidor de réplica de destino.

Total de archivos suprimidos

El número total de archivos que se han suprimido en el servidor de réplica de destino.

Total de archivos no suprimidos debido a errores

El número total de archivos de copia de seguridad, archivado y gestionados por espacio que no se han suprimido en el servidor de réplica de destino debido a errores.

Total de archivos para actualizar

El número total de archivos que se van a actualizar en el servidor de réplica de destino. Cuando los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Total de archivos actualizados

El número total de archivos que se han actualizado en el servidor de réplica de destino.

Total de archivos no actualizados debido a errores

El número total de archivos de copia de seguridad, archivado y gestionados por espacio que no se han actualizado en el servidor de réplica de destino debido a errores.

Total de bytes para replicar (MB)

El número total de bytes que se replican en el servidor de réplica de destino.

Total de bytes replicados (MB)

El número total de bytes que se han replicado en el servidor de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Total de bytes transferidos (MB)

El número total de bytes que se han transferido al servidor de réplica de destino.

Para los archivos almacenados en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el valor en este campo incluye el número de bytes en el archivo original antes de que se hayan eliminado las extensiones duplicadas. Si todavía hay extensiones duplicadas en el servidor de réplica de destino, el número de bytes en el archivo original es mayor que el número de bytes transferidos.

Total de bytes no replicados debido a errores (MB)

El número total de bytes que se han omitido porque el servidor de réplica de origen no ha podido transferirlos al servidor de réplica de destino.

Total de bytes aún no replicados (MB)

El número total de bytes que no se han transferido todavía al servidor de réplica de destino.

Porcentaje de finalización estimado

El porcentaje de terminación estimado basado en el número de bytes.

Tiempo restante estimado

El tiempo estimado que queda antes de que el proceso de réplica de nodo se haya completado.

Tiempo de finalización estimado

La hora estimada en que finalizará el proceso de réplica de nodo.

Tabla 1. Mandatos relacionados con QUERY REPLICATION

Mandato	Descripción
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLETENTION	Especifica el periodo de retención de los registros de historial de réplicas.

QUERY REPLNODE (Mostrar información sobre el estado de réplica de un nodo de cliente)

Utilice este mandato para mostrar el número de archivos almacenados para cada espacio de archivos replicado. Se muestra información sobre los espacios de archivo para cada nodo de cliente configurado para la réplica.

Se configura un nodo de cliente para la réplica si está activado o desactivado.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
Query REPLNode-----nombre_nodo-----+----->
'-nombre_servidor_destino-'<
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nodo de cliente que es propietario de los archivos sobre los que desea información. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas. No utilice espacios intercalados. Puede utilizar caracteres comodín

para especificar varios nombres.

No se muestra la información sobre los nodos de cliente que coinciden con los criterios de archivo, pero que no están configurados para la réplica.

nombre_servidor_destino

Especifica el nombre del servidor de réplica que se va a consultar para obtener información de réplica. Este parámetro es opcional. Si no especifica un valor para este parámetro, se consulta el servidor que es el destino predeterminado para los datos replicados.

Como valor para este parámetro, también puede especificar un servidor que haya sido previamente un destino de los datos replicados.

Los nodos de cliente definidos en un servidor de réplica pueden ser el origen o el destino de los datos replicados. Para determinar si un nodo de cliente en particular está enviando o recibiendo datos, emita el mandato QUERY NODE. Busque el valor *Send* o *Receive* en el campo Modalidad de réplica de la salida.

Para visualizar el nombre del servidor de réplica de destino activo, emita el mandato QUERY STATUS y busque el nombre en el campo Servidor de réplica de destino.

Ejemplo: listar los archivos de nodo de cliente en un servidor de réplica de origen y un servidor de réplica de destino

El nombre del nodo de cliente es NODE1.

```
query replnode *
```

Nodo Nombre	Tipo	Espacio de archivos Nombre	Archivos	FSID Servidor	Archivos en Servidor	Réplica Servidor (1)	Archivos en Servidor (1)
NODE1	SpMg	/hmsmfs	1	1			
NODE1	Bkup	/lspace2	2	27			
NODE1	Arch	/lspace2	2	22	TGTSRV	22	
NODE1	Bkup	/lspace	3	18.096			
NODE1	Arch	/lspace	3	61.150	TGTSRV	61.150	
NODE2							

El número de archivos visualizados para los servidores de réplica puede ser diferente por los motivos siguientes:

- La salida del mandato QUERY REPLNODE visualiza el número de archivos obtenidos de la tabla de ocupación. La tabla de ocupación sólo contiene archivos con una longitud mayor que cero. Los archivos que tienen una longitud de 0 y que se han replicado no se reflejan en esta salida.
- Si sólo se replican datos activos en el servidor de destino, el número de archivos visualizados para el servidor de origen será mayor que el número de archivos visualizados en el servidor de destino. El motivo de esta diferencia es que el servidor de réplica de origen tiene datos activos e inactivos y el servidor de destino sólo tiene datos activos.
- Un nodo de cliente puede tener datos exportados desde el servidor de réplica de origen e importados al servidor de réplica de destino. Si se han sincronizado los datos y el nodo de cliente también ha almacenado datos en el servidor de réplica de destino, el número de archivos en el servidor de réplica de destino será mayor que el número de archivos almacenados como resultado de las operaciones de exportación e importación y de la réplica.
- Cuando se replican datos de nodo desde un servidor de origen anterior a la versión 7.1 a un servidor de destino de la versión 7.1 o posterior, los archivos más grandes de 10 GB se dividen en archivos más pequeños si el parámetro SPLITLARGEOBJECTS de la definición de nodo está definido a *Yes*. Cada uno de estos archivos divididos se cuenta en el servidor de destino.

Descripciones de los campos

Nombre del nodo

El nombre del nodo de cliente que es propietario de los archivos.

Tipo

El tipo de datos. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica. En la salida de ejemplo, NODE2 está configurado para la réplica, pero no tiene datos de copia de seguridad, archivado o gestionados por espacio.

Son posibles los siguientes valores:

Arch

Datos de archivado

C.S.

Datos de copia de seguridad

G.E.

Datos que IBM Spectrum Protect ha migrado para los clientes de gestión de espacio

Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

FSID

El identificador de espacio de archivos del espacio de archivos. El servidor asigna un FSID único cuando un espacio de archivo se almacena inicialmente en el servidor. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Archivos en el servidor

El número de archivos de copia de seguridad, archivado y gestionados por espacio en el servidor en el que se emite este mandato. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Servidor de réplica (1)

El nombre del servidor de réplica para el que se está consultando información. Si este campo está en blanco, pueden existir una o varias de las condiciones siguientes:

- El espacio de archivos del nodo en el servidor de réplica donde se ha emitido el mandato no tiene ningún dato.
- El nodo de cliente no está definido en el servidor de réplica (1).
- El nodo de cliente está definido en el servidor de réplica (1), pero el nodo no está configurado para la réplica.
- El espacio de archivos correspondiente en el servidor de réplica (1) no tiene datos o el espacio de archivos no está definido.

Archivos en el servidor (1)

El número de archivos para el tipo de datos almacenados en el servidor de réplica de destino. Este campo puede estar en blanco. Si lo está, pueden existir una o varias de las condiciones siguientes:

- El servidor de réplica (1) no tiene datos.
- El nodo de cliente no está definido en el servidor de réplica (1).
- El nodo de cliente está definido en el servidor de réplica (1), pero el nodo no está configurado para la réplica.
- El espacio de archivos correspondiente en el servidor de réplica (1) no tiene datos o el espacio de archivos no está definido.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY REPLNODE

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.

Nombre de regla de réplica: ALL_DATA_HIGH_PRIORITY
Servidor de réplica de destino:
Sólo activos: No
Activado: Si

Descripciones de los campos

Nombre de norma de réplica

Especifica el nombre de la regla que se ha consultado.

Servidor de réplica destino

Especifica el nombre del servidor de réplica de destino.

Sólo activos

Especifica si la regla se aplica sólo a los datos de copia de seguridad activos. Son posibles los siguientes valores:

Si

Especifica que sólo se replican los datos de copia de seguridad activos para los espacios de archivos a los que se ha asignado esta regla.

No

Especifica que se replican todos los datos de copia de seguridad para los espacios de archivos a los que se ha asignado esta regla.

Habilitado

Especifica si la regla está activada o desactivada. Son posibles los siguientes valores:

Si

Especifica que la regla está activada para la réplica. Los datos en los espacios de archivos a los que se ha asignado la regla se replican.

No

Especifica que la regla no está activada para la réplica. Los datos en los espacios de archivos a los que se ha asignado la regla no se replican.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY REPLRULE

Mandato	Descripción
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.

QUERY REPLSERVER (Consultar un servidor de réplica)

Utilice este mandato para ver información sobre todos los servidores de réplica que conoce el servidor. El resultado de este mandato incluye información del servidor para el servidor desde donde se ha emitido el mandato. El mandato indica si una definición de servidor de réplica se suprime como resultado de un mandato REMOVE REPLSERVER.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query REPLServer-+-----+-----<<
                    .-*-----
                    '-nombre_servidor-'
```

Ejemplo: visualizar estadísticas de resumen acerca de todos los servidores de réplica

Visualizar información sobre el servidor de réplica. Emita el mandato desde el servidor de réplica de origen o de destino:

```
query replserver *
```



```

ID exclusivo global de réplica: 4d.83.fc.30.67.c1.11.e1.b8.
                                40.f0.de.f1.5e.f1.89
    Nombre de servidor: Server1
    Última réplica:
    Pulsación:
Dirección de alto nivel de migración tras error: server1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas:

ID exclusivo global de réplica: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
    Nombre de servidor: DRServer1
    Última réplica: 30/06/2012 08:16:30
    Pulsación: 07/09/2012 22:15:22
Dirección de alto nivel de migración tras error: drserver1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas: On

ID exclusivo global de réplica: 90.4f.53.b0.8e.cb.11.e3.a8.
                                2f.00.14.5e.55.b3.67
    Nombre de servidor: DRSERVER2
    Última réplica: 01/04/2014 12:38:28
    Pulsación: 29/05/2014 11:15:44
Dirección de alto nivel de migración tras error: drserver2.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error:
Supresión en curso: No
                                Políticas heterogéneas: Off

```

Ejemplo: visualizar estadísticas de resumen acerca de un servidor de réplica específico

Visualizar información sobre el servidor de réplica DRServer1. Emita el mandato desde el servidor de réplica de origen o de destino:

```
query replserver drserver1
```

```

ID exclusivo global de réplica: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
    Nombre de servidor: DRServer1
    Última réplica: 30/06/2012 08:16:30
    Pulsación: 07/09/2012 22:15:22
Dirección de alto nivel de migración tras error: drserver1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas: On

```

Parámetros

nombre_servidor

Especifica el nombre del servidor de réplica a consultar. Puede utilizar caracteres comodín para especificar este nombre. Se consultarán todos los servidores coincidentes. Si no especifica un valor para este parámetro, se consultarán todos los servidores. El parámetro es opcional.

Descripciones de los campos

ID exclusivo global de réplica

El identificador exclusivo para el servidor de IBM Spectrum Protect. Los valores para el ID exclusivo global de réplica se crea cuando un servidor se utiliza por primera vez en un proceso de réplica.

Consejo: El ID que aparece en el campo ID exclusivo global de duplicación no es el mismo valor que el del ID en el campo ID exclusivo global de máquina que se muestra en el mandato QUERY STATUS.

Nombre servidor

Nombre del servidor de réplica.

Última réplica

La fecha del proceso de réplica último que utiliza el servidor.

Pulsación

La última vez que el servidor ha finalizado una sesión de comunicación de prueba satisfactoria.

Número de puerto TCP de migración tras error

El activo Transmission Control Protocol (TCP) de puerto de cliente en el servidor de réplica que se utiliza para las conexiones de cliente. Si el cliente está configurado para TCP, el puerto se utiliza para conectar con el servidor de migración tras error.

Número de puerto SSL de migración tras error

El puerto SSL activo en el servidor de réplica que se utiliza para las conexiones de cliente. Si el cliente está configurado para SSL, el puerto se utiliza para conectar con el servidor de migración tras error.

Dirección de alto nivel de migración tras error

La dirección de alto nivel que el cliente utiliza para conectar con el servidor de réplica durante la migración tras error.

Supresión en curso

Especifica si se ha emitido un mandato REMOVE REPLSERVER para este servidor de réplica y si todavía está en curso. Son posibles los siguientes valores:

Sí

La supresión del servidor de réplica está en curso.

No

La supresión de este servidor de réplica no está en curso.

Políticas distintas

Especifica si las políticas que están definidas en el servidor de réplica de destino están habilitadas. Son posibles los siguientes valores:

Activo

Las políticas en el servidor de réplica de destino gestionan datos de nodo cliente replicados.

Inactivo

Las políticas en el servidor de réplica de origen gestionan datos de nodos cliente replicados.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY REPLSERVER

Mandato	Descripción
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	Elimina un nodo de la réplica.
REMOVE REPLSERVER (Eliminar un servidor de réplica)	Elimina un servidor de la réplica.

QUERY REQUEST (Consultar una o más peticiones de montaje pendientes)

Utilice el mandato QUERY REQUEST para mostrar información acerca de una o varias solicitudes de montaje pendientes. El servidor realiza peticiones al administrador para llevar a cabo una acción, como insertar un volumen de cinta en una biblioteca después de haberse emitido un mandato CHECKIN LIBVOL.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query REQuest--+-+-----+----->>  
                    '-numero_petición-'
```

Parámetros

numero_petición

Especifica el número de identificación de la petición de montaje pendiente. Este parámetro es opcional. El valor predeterminado son todas las peticiones de montaje pendientes.

Ejemplo: obtener una lista de todas las peticiones de montaje pendientes

Visualizar información acerca de todas las peticiones de montaje pendientes después de haberse emitido un mandato CHECKIN LIBVOL.

```
query request
```

Salida de una biblioteca manual

 Sistemas operativos AIX

ANR8352I Peticiones pendientes:
 ANR8326I 001: Montar el volumen 8MM EXP001 R/W
 en la unidad 8MM.1 (/dev/mt0) de la biblioteca
 MANUALLIB en los próximos 60 minutos.

 Sistemas operativos Linux

ANR8352I Peticiones pendientes:
 ANR8326I 001: Montar el volumen 8MM EXP001 R/W
 en la unidad 8MM.1 (/dev/mt0) de la biblioteca
 MANUALLIB en los próximos 60 minutos.

 Sistemas operativos Windows

ANR8352I Peticiones pendientes:
 ANR8326I 001: Montar el volumen GENERICTAPE EXP001 R/W
 en la unidad 8MM.1 (mt3.0.0.0) de la biblioteca
 MANUALLIB en los próximos 60 minutos.

Salida de una biblioteca automatizada

 Sistemas operativos AIX  Sistemas operativos Windows

ANR8352I Peticiones pendientes:
 ANR8306I 001: Insertar el volumen LTO 133540L5 R/W en la ranura con
 número elemento 31 de la biblioteca LTOLIB en los próximos 60 minutos; emitir
 'REPLY' juntamente con ID de solicitud cuando esté listo.

 Sistemas operativos Linux

ANR8352I Peticiones pendientes:
 ANR8306I 001: Insertar el volumen 3590 133540 R/W en la ranura
 con el elemento
 número 31 de la biblioteca 3590LIB en los próximos
 60 minutos; emitir 'REPLY'
 juntamente con la petición ID cuando
 esté listo.

Mandatos relacionados

Tabla 1. Mandatos relacionados para QUERY REQUEST

Mandato	Descripción
CANCEL REQUEST	Cancela las peticiones pendientes de montaje de volúmenes.
REPLY	Permite que una petición siga procesándose.

QUERY RESTORE (Consultar sesiones de restauración reiniciables)

Utilice este mandato para visualizar la información sobre las sesiones de restauración reiniciables.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query--REStore--+-+-----+-----+-----+-----+----->
                    '-nombre_nodo-' '-nombre_espacio_archivos-'

    .-Format-----Standard----- .-NAMEType-----SERVER-----.
>>+-----+-----+-----+-----+-----+-----+----->>
    '-Format-----+Standard+-' '-NAMEType-----+SERVER--+-'
                    '-Detailed-'                               +-UNICODE+-
                    '-FSID-----'
```

Parámetros

nombre_nodo

Especifica el nombre del nodo cliente que se consultará. Este parámetro es opcional. Si no especifica un valor, se visualizarán todos los nodos cliente con sesiones de restauración reiniciables. Debe especificar un valor para este parámetro si especifica un nombre de espacio de archivos.

nombre_espacio_archivos

Especifica el nombre del espacio de archivos que se consultará. Este parámetro es opcional. Si no especifica un valor, se compararán todos los espacios de archivos para el nodo especificado.

Para un servidor que tenga clientes que admiten Unicode, es posible que deba utilizar el servidor para que éste convierta el nombre del espacio de archivos que especifica. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre especificado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para conocer los detalles.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS 9, Macintosh OS X y NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

Ejemplo: visualizar una sesión de restauración reiniciable en un nodo cliente específico

Visualizar información detallada sobre el nodo cliente JAMES asociado al espacio de archivos DRIVE_F_R. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query restore james drive_f_r format=detailed
```

```
Número sesión: -1
Estado restauración: Reiniciable
Minutos transcurridos: 2
Nombre nodo: JAMES
FSID: 1
Nombre espacio archivos: DRIVE_F_R:
Espec. archivo: /RESTORE/TESTDIRF\
```

Descripciones de los campos

Número de sesión

Especifica el número de sesión de la sesión de restauración reanunciable. El número de las sesiones de restauración activas es el mismo número que se visualiza en el mandato QUERY SESSION. Para las sesiones de restauración que están en estado reiniciable, se visualiza un número negativo como número de sesión. Cualquier número de sesión que se visualice en la salida de QUERY RESTORE puede especificarse desde la salida de QUERY RESTORE.

Estado restauración

- Activo: Especifica que la sesión de restauración está activa, restaurando los archivos en el cliente.
- Reiniciable: Especifica que la sesión de restauración no se ha ejecutado correctamente y que puede reiniciarse desde donde ha quedado interrumpida.

Minutos transcurridos

Especifica el número de minutos desde que se ha arrancado la sesión de restauración. Todas las sesiones de restauración reiniciables con un tiempo transcurrido mayor que el valor de la opción del servidor RESTOREINTERVAL pueden suprimirse automáticamente de la base de datos del servidor cuando sea necesario, o durante el proceso de caducidad. Si el tiempo transcurrido es inferior al valor de RESTOREINTERVAL, esta entrada sólo puede suprimirse (y desbloquearse el espacio de archivos) mediante la emisión del mandato CANCEL RESTORE y la reducción del valor de RESTOREINTERVAL.

Node Name

Especifica el nodo asociado a la sesión de restauración reiniciable.

FSID

Especifica el identificador del espacio de archivos.

Filespace Name

Especifica el espacio de archivos asociado a la sesión de restauración reiniciable.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Especificación de archivo

Indica la especificación de archivo utilizada en la operación de restauración. Debe indicarse la misma especificación de archivo si se va a reiniciar una operación de restauración que no se ha podido ejecutar desde el punto en que se detuvo.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY RESTORE

Mandato	Descripción
CANCEL RESTORE	Cancela una sesión de restauración reiniciable.

QUERY RPFCONTENT (Consultar el contenido del archivo del plan de recuperación almacenado en un servidor de destino)

Utilice este mandato para visualizar el contenido de un archivo del plan de recuperación almacenado en un servidor de destino (es decir, cuando el parámetro DEVCLASS se ha especificado en el mandato PREPARE). Puede emitir este mandato desde el servidor que ha creado el archivo (el servidor de origen) o desde el servidor que almacena el archivo del plan de recuperación (el servidor de destino). Este mandato no se puede emitir en la consola del servidor.

La salida se puede retardar si el archivo está en cinta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Query RPFContent--nombre_archivo_plan----->
>--+DEVclass----nombre_clase_dispositivo+-----<
  '-NODENAME----nombre_nodo-----'
```

Parámetros

nombre_archivo_plan (Obligatorio)

Especifica el nombre del archivo del plan de recuperación que se ha de consultar. El formato del nombre de archivo es nombreservidor.aaaammdd.hhmmss. Para ver los nombres de los archivos existentes, emita el mandato QUERY RPFIL.

DEVclass

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear el archivo del plan de recuperación. Los caracteres comodín no están permitidos.

Especifique este parámetro cuando:

- Desea visualizar el contenido del archivo del plan de recuperación creado para este servidor.
- Emita este mandato en el mismo servidor en el que se ha emitido el mandato PREPARE (el servidor de origen).
- Se haya utilizado el nombre de clase de dispositivo especificado en el mandato PREPARE que ha creado el archivo del plan de recuperación.

NODENAME

Especifica el nombre de nodo, registrado en el servidor de destino, del servidor de origen que ha creado el archivo del plan de recuperación. Los caracteres comodín no están permitidos.

Especifique este parámetro cuando:

- Desea visualizar el contenido del archivo del plan de recuperación que estaba almacenado en servidor.
- Emita este mandato para el servidor que era el destino del mandato PREPARE que ha creado el archivo del plan de recuperación.
- El nombre de nodo especificado esté registrado en este servidor con un tipo de nodo de SERVER.
- El servidor de IBM Spectrum Protect que ha creado el archivo del plan de recuperación no esté disponible.

Ejemplo: visualizar el plan de recuperación del servidor de origen

En el servidor origen, visualizar el contenido de un archivo del plan de recuperación que se ha creado para este servidor el 19 de marzo de 1998 a las 6:10 A.M. El mandato PREPARE especifica la clase de dispositivo REMOTE. La salida de este mandato es el contenido completo del archivo del plan de recuperación.

```
query rpfcontent branch1.19980319.061000 devclass=remote
```

Ejemplo: visualizar el plan de recuperación del servidor de destino

En el servidor de destino, visualizar el contenido de un archivo del plan de recuperación que se ha almacenado en este servidor el 19 de marzo de 1998 a las 6:10 A.M. El servidor que ha creado el archivo está inscrito en el servidor destino como el nodo denominado POLARIS y tiene el tipo de nodo SERVER. La salida de este mandato es el contenido completo del archivo del plan de recuperación.

```
query rpfcontent branch1.19980319.061000 nodename=polaris
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY RPFCONTENT

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFIL	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.

Información relacionada:

[🔗](#) Archivo del plan de recuperación tras siniestro

QUERY RPFIL (Consultar la información del archivo del plan de recuperación almacenado en un servidor de destino)

Utilice este mandato para visualizar la información sobre los archivos del plan de recuperación almacenados en un servidor destino. Puede emitir este mandato desde el servidor que ha creado el archivo (el servidor origen) o desde el servidor que almacena el archivo del plan de recuperación (el servidor destino).

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query RPFile--+-DEVclass-----nombre_clase_dispositivo+----->
      '-NODEName-----nombre_nodo-----'

.-Source-----DBBackup-----.-Format-----Standard-----
>--+-----+-----+-----+-----+-----+-----+-----+----->>
  '-Source-----+-DBBackup-----+' '-Format-----+-Standard-+-'
      '-DBSnapshot-'                '-Detailed-'
```

Parámetros

DEVclass

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear los archivos del plan de recuperación. Utilice este parámetro si ha iniciado la sesión en el servidor que ha creado el archivo del plan de recuperación. Puede utilizar caracteres comodín en el nombre de clase de dispositivo. En la consulta se incluirán todos los archivos del plan de recuperación que se han creado con la clase de dispositivo especificada.

NODEName

Especifica el nombre de nodo, registrado en el servidor destino, del servidor origen que ha creado los archivos del plan de recuperación. Utilice este parámetro si ha iniciado la sesión en el servidor destino. Puede utilizar este parámetro si el servidor origen no está disponible. Puede utilizar caracteres comodín para especificar el nombre de nodo. En esta consulta se incluyen todos los objetos de archivo que están almacenados con el nombre de nodo especificado.

Source

Especifica el tipo de copia de seguridad de base de datos indicada al preparar el archivo del plan de recuperación. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Los valores posibles son:

DBBackup

El archivo del plan de recuperación se preparó con copias de seguridad completas e incrementales especificadas.

DBSnapshot

El archivo del plan de recuperación se preparó con las copias de seguridad de instantánea de base de datos especificadas.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Visualiza información parcial para el archivo del plan de recuperación.

Detailed

Visualiza toda la información para el archivo del plan de recuperación.

Ejemplo: visualizar información detallada acerca de los planes de recuperación

Visualizar los archivos de plan de recuperación que se han creado para este servidor empleando la clase de dispositivo especificada. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query rpfile devclass=* format=detailed

Nombre archivo plan recuperación: ALASKA.20000406.170423
      Nombre nodo: BRANCH1
      Nombre clase dispositivo: REMOTE
Tipo archivo plan recuperación: RPFILE
      Nombre clase gestión: STANDARD
Tamaño archivo plan recuperación: 16.255 Bytes
  Marca supresión: Sí
      Fecha supresión: 06/12/2000 13:05:31

Nombre archivo plan recuperación: ALASKA.20000407.170845
      Nombre nodo: BRANCH1
      Nombre clase dispositivo: REMOTE
Tipo archivo plan recuperación: RPFSSNAPSHOT
      Nombre clase gestión: STANDARD
Tamaño archivo plan recuperación: 16.425 Bytes
  Marca supresión: No
      Fecha supresión:
```

Ejemplo: visualizar una lista de los planes de recuperación para un nombre de nodo específico

Visualizar una lista de todos los objetos de archivo del plan de recuperación que están almacenados con el nombre de nodo especificado (TIPO=SERVER). Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query rpfile nodename=branch1
```

Nombre archivo plan recuperación	Nombre nodo	Nombre clase dispositivo
ALASKA.19980406.170423	BRANCH1	REMOTE
ALASKA.19980407.170845	BRANCH1	REMOTE

Descripciones de los campos

Nombre del archivo del plan de recuperación

El nombre del archivo del plan de recuperación.

Node Name

El nombre del nodo que está registrado con el servidor destino y se utiliza para almacenar los objetos de archivo del plan de recuperación.

Nombre clase dispositivo

El nombre de clase de dispositivo que está definido en el servidor origen y se utiliza para crear los archivos del plan de recuperación.

Tipo de archivo del plan de recuperación

Indica el tipo de archivo del plan de recuperación:

RPFIL

El plan presupone copias de seguridad completas e incrementales.

RPFsnapshot

El plan presupone copias de seguridad de instantánea de base de datos.

Nombre clase gestión

El nombre de la clase de gestión a la que el archivo del plan de recuperación está asociado en el servidor destino.

Tamaño del archivo del plan de recuperación

Tamaño estimado del objeto archivo del plan de recuperación del servidor destino.

Marcado para suprimir

Si el objeto que contiene el archivo del plan de recuperación se ha suprimido del servidor origen y se ha marcado para suprimir en el servidor destino si el período de gracia no ha caducado. Los valores posibles son:

Sí

El objeto se marca para suprimirlo.

No

El objeto no se marca para suprimirlo.

Fecha supresión

Fecha en la que el objeto se ha suprimido del servidor origen y se ha marcado para supresión en el servidor destino. Este campo está en blanco si el objeto no está marcado para supresión.


Mandatos relacionados


Tabla 1. Mandatos relacionados con QUERY RPFIL


Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.

QUERY SAN (Consultar los dispositivos de la SAN)

Utilice este mandato para obtener información acerca de los dispositivos que se pueden detectar en una red de área de almacenamiento (SAN) para poder configurar IBM Spectrum Protect para un traspaso de datos libre de LAN.

 Sistemas operativos AIX El mandato QUERY SAN requiere que libhbaapi.a dé soporte a la API de adaptador de bus de host (HBA) SNIA común. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBAAPI común SNIA.

 Sistemas operativos Windows El mandato QUERY SAN requiere que hbaapi.dll dé soporte a la API del adaptador de bus de host (HBA) común SNIA. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBAAPI común SNIA.

 Sistemas operativos Linux El mandato QUERY SAN requiere que libhaapi.so dé soporte a la API de adaptador de bus de host (HBA) SNIA común. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBAAPI común SNIA.

Puede que el mandato QUERY SAN no muestre todos los dispositivos si la opción del servidor SANDISCOVERY no está establecida en ON.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-Type-----Any----- .
>>-Query SAN-----+----->
      '-Type-----+Any-----+'
                +-DRive---+
                '-LIBRARY-'

.-Format-----Standard----- .
>-----+-----<
      '-Format-----+Standard-+-'
                '-Detailed-'
```

Parámetros

Type

Especifica el tipo de dispositivo que se visualiza. Este parámetro es opcional. El valor predeterminado es Any. Los valores posibles son:

Any

Especifica que se puede visualizar cualquier dispositivo que se detecte en SAN.

DRive

Especifica que solamente se visualizarán los dispositivos de unidad.

LIBRARY

Especifica que solamente se visualizarán los dispositivos de biblioteca.

Format

Especifica el tipo de información que se visualiza. Este parámetro es opcional. El valor predeterminado es Standard. Los valores posibles son:

Standard

Especifica que la información visualizada está resumida.

Detailed

Especifica que se visualizará toda la información.

Consejo: Puede que la salida no visualice el número de serie del dispositivo. Si esto es así, busque en la parte posterior del dispositivo o póngase en contacto con el fabricante del dispositivo.

Ejemplo: obtener una lista de los dispositivos de unidad

Visualizar información resumida de los dispositivos de unidad de una SAN. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query san type=drive
```

Tipo dispo.	Proveedor	Producto	Serie	Dispositivo
-----	-----	-----	-----	-----
LIBRARY	STK	L180		MPC01000128 /dev/smc1
DRIVE	STK	9840D	331001017229	/dev/rmt3
DRIVE	Quantum	DLT4000	JF62806275	/dev/rmt4
DRIVE	Quantum	DLT4000	JP73213185	/dev/rmt5
DRIVE	STK	9840D	331000028779	/dev/rmt6

Ejemplo: visualizar información de dispositivo de unidad

Visualizar información detallada de todos los dispositivos de unidad de una SAN. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query san type=drive format=detailed
```

```
Tipo dispositivo:    DRIVE
Proveedor:         IBM
Producto:         03570B02
Número de serie:
  Dispositivo:     mt10.2.0.3
Transportador de datos: No
Nodo WWN:         5005076206039E05
Puerto WWN:       5005076206439E05
  LUN:            0
Puerto SCSI:      3
Bus SCSI:         0
Destino SCSI:     10
```

Descripciones de los campos

Tipo dispositivo

El tipo de dispositivo que se está visualizando.

Proveedor

El nombre del proveedor del dispositivo.

Producto

El nombre del producto que asigna el proveedor.

Número de serie

El número de serie del dispositivo.

Dispositivo

El nombre del archivo de dispositivo especial.

Transportador de datos

Si el dispositivo es un transportador de datos.

WWN de nodo

Nombre de ámbito mundial del dispositivo.

WWN de puerto

Nombre de ámbito mundial del dispositivo, que es específico del puerto con el que se ha conectado el dispositivo.

LUN

El número de unidad lógica del dispositivo.

Puerto de SCSI

El puerto del adaptador de bus de host de canal de fibra (o SCSI)

Bus de SCSI

El bus de la tarjeta adaptadora del bus de host.

Destino de SCSI

El número de destino del dispositivo.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SAN

Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.

QUERY SCHEDULE (Consultar planificaciones)

Utilice este mandato para visualizar información acerca de una o varias planificaciones.

El mandato QUERY SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones del cliente o a los mandatos de administración. La sintaxis y los parámetros de cada operación se definen por separado. Algunas opciones de la visualización de la consulta estarán en blanco, en función de si el estilo de planificación es clásico o mejorado.

Detailed

Especifica que se visualizará información detallada acerca de las planificaciones.

El formato estándar muestra un espacio en blanco en la columna de periodo y un asterisco en la columna de día en las planificaciones mejoradas. Para visualizar información completa acerca de una planificación mejorada, emita FORMAT=DETAILED.

Ejemplo: obtener una lista de las planificaciones de un dominio de políticas específico

Visualizar todas las planificaciones que pertenecen al dominio de políticas EMPLOYEE_RECORDS. Consulte el apartado Descripciones de los campos: planificaciones de un dominio de políticas específico para obtener las descripciones de los campos.

```
query schedule employee_records
```

El formato estándar muestra un espacio en blanco en la columna de periodo y un asterisco en la columna de día en las planificaciones mejoradas. Para visualizar información completa acerca de una planificación mejorada, emita FORMAT=DETAILED.

Domain	* Schedule Name	Action	Start Date/Time	Duration	Period	Day
EMPLOYEE_RECORDS	WEEKLY_BACKUP	Inc Bk	2004.06.04 17.04.20	1 H	1 D	Any
EMPLOYEE_RECORDS	EMPLOYEE_BACKUP	Inc Bk	2004.06.04 17.04.20	1 H		(*)

Descripciones de los campos: planificaciones de un dominio de políticas específico

Domain

Especifica el nombre del dominio de políticas al que pertenece la planificación especificada.

* (asterisco)

Especifica si ha caducado la planificación correspondiente. Si existe un asterisco en esta columna, ha caducado la planificación correspondiente.

Schedule Name

Especifica el nombre de la planificación.

Acción

Especifica la acción que se produce cuando se procesa esta planificación.

Fecha/hora inicio

Especifica la fecha y hora de inicio de esta planificación.

Duración

Especifica la duración del margen de puesta en marcha de esta planificación.

Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que DAYOFWEEK=ANY). La columna está en blanco en las planificaciones mejoradas.

Día

Especifica el día de la semana en que se inician los márgenes de puesta en marcha de esta planificación. La columna contiene un asterisco en las planificaciones mejoradas.

Ejemplo: visualizar información detallada acerca de las planificaciones de cliente

Desde un servidor gestionado, visualizar información detallada sobre las planificaciones de cliente. Consulte el apartado Descripciones de los campos: información detallada acerca de las planificaciones de cliente para obtener las descripciones de los campos.

```
query schedule * type=client format=detailed
```

```
Nombre dominio políticas: ADMIN_RECORDS
Nombre planificación: ADMIN_BACKUP
Descripción:
  Acción: Backup
  Subacción: vApp
  Opciones:
  Objetos:
  Prioridad: 5
Fecha/hora inicio: 04/06/2013 17.04.20
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Clásico
Período: 1 día(s)
```

```

Día semana: Cualquiera
Mes:
Día del mes:
Semana del mes:
Caducidad:
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/hora de la última actualización: 06/04/2013 17.51.49
Perfil de gestión: ADMIN_INFO

Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre planificación: EMPLOYEE_BACKUP
Descripción:
Acción: Incremental
Subacción:
Opciones:
Objetos:
Prioridad: 5
Fecha/hora inicio: 2004.06.04 17.04.33
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Mejorado
Periodo:
Día semana: Cualquiera
Mes: Mar,Jun,Nov
Día del mes: -14,14,22
Semana del mes: Última
Caducidad:
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/hora última actualización: 2004.06.04 17.18.30
Perfil de gestión: EMPLOYEE

```

Descripciones de los campos: información detallada acerca de las planificaciones de cliente

Nombre dominio políticas

Especifica el nombre del dominio de políticas.

Schedule Name

Especifica el nombre de la planificación.

Descripción

Especifica la descripción de la planificación.

Acción

Especifica el tipo de acción que se produce cuando se ejecuta esta planificación. Consulte el mandato DEFINE SCHEDULE para obtener un listado de las acciones.

Subacción

Especifica que el tipo de operación identificado por el parámetro ACTION se debe planificar. Consulte el mandato DEFINE SCHEDULE para obtener un listado de las subacciones.

Opciones

Especifica las opciones que se suministran al mandato DSMC cuando se procesa la planificación.

Objetos

Especifica los objetos para los que se realiza la acción especificada.

Prioridad

Especifica el valor de prioridad de la planificación.

Fecha/hora inicio

Especifica la fecha y hora de inicio de la planificación.

Duración

Especifica la duración del margen de puesta en marcha de la planificación.

Tiempo máximo de ejecución(Minutos)

Especifica el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Estilo de planificación

Especifica si se utilizan reglas de planificación clásicas o mejoradas.

Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que DAYOFWEEK=ANY). No se visualiza para las planificaciones de sintaxis mejoradas.

Día de la semana

Especifica el día de la semana en que se inician los márgenes de puesta en marcha de esta planificación. Mediante la utilización de un formato estándar, visualiza un asterisco en el campo del día de la semana para las planificaciones mejoradas.

Mes

Especifica los meses durante los cuales se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Día del mes

Especifica los días durante los cuales se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Semana del mes

Especifica las semanas (primera, segunda, tercera, cuarta o última) del mes durante el cual se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Caducidad

Especifica la fecha y hora en la que caduca esta planificación. Si esta columna está en blanco, la planificación no caducará.

Última actualización por (administrador)

Especifica el nombre del administrador que ha actualizado por última vez la planificación. Si este campo contiene \$\$CONFIG_MANAGER\$\$, la planificación está asociada a un dominio que gestiona el gestor de configuración.

Fecha/hora de la última actualización

Especifica la fecha y hora en que se ha actualizado por última vez la planificación.

Perfil de gestión

Especifica el perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de esta planificación.

QUERY SCHEDULE (Consultar una planificación de administración)

Utilice este mandato para visualizar información acerca de una o varias planificaciones de administración.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----  
>>-Query SCHEDULE--+-+----->  
      '-nombre_planificación-'  
  
      .-Format----Standard----.  
>--Type----Administrative--+-+-----<  
      '-Format----+Standard+-'  
      '-Detailed-'
```

Parámetros

nombre_planificación

Especifica el nombre de la planificación que se consultará. Puede utilizar un carácter comodín para especificar este nombre.

Type=Administrative (Necesario)

Especifica que la consulta visualiza las planificaciones de mandato de administración.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial acerca de las planificaciones.

Detailed

Especifica que se visualizará información detallada acerca de las planificaciones.

El formato estándar presenta una columna de periodo en blanco y un asterisco en la columna de día en las planificaciones mejoradas. Emita el mandato FORMAT=DETAILED para visualizar la información completa sobre una planificación mejorada.

Ejemplo: visualizar información detallada acerca de planificaciones de mandatos de administración

Desde un servidor gestionado, visualizar información detallada sobre las planificaciones de mandato de administración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query schedule * type=administrative  
format=detailed
```

```
Nombre planificación: BACKUP_ARCHIVEPOOL  
Descripción:  
Mandato: backup db
```

Prioridad: 5
Fecha/hora inicio: 2004.06.04 16.57.15
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Clásico
Período: 1 día(s)
Día semana: Cualquiera
Mes:
Día del mes:
Semana del mes:
Caducidad:
Activo: No
Última actualización por (administrador): \$\$CONFIG MANAGER\$\$
Fecha/hora última actualización: 2004.06.04 17.51.49
Perfil de gestión: ADMIN_INFO

Nombre planificación: MONTHLY_BACKUP
Descripción:
Mandato: q status
Prioridad: 5
Fecha/hora inicio: 2004.06.04 16.57.14
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Mejorado
Período:
Día de la semana: Mar, Jue, Vie
Mes: Ago, Nov
Día del mes:
Semana del mes: Segunda, Tercera
Caducidad:
Activo: No
Última actualización por (administrador): \$\$CONFIG MANAGER
Fecha/hora última actualización: 2004.06.04 17.51.49
Perfil de gestión: ADMIN_INFO

Descripciones de los campos

Schedule Name

Especifica el nombre de la planificación.

Descripción

Especifica la descripción de la planificación.

Mandato

Especifica el mandato que se ha planificado.

Prioridad

Especifica el valor de prioridad de esta planificación.

Fecha/hora inicio

Especifica la fecha y hora de inicio de esta planificación.

Duración

Especifica la duración del margen de puesta en marcha.

Tiempo máximo de ejecución(Minutos)

Especifica el número de minutos durante los cuales los procesos de servidor que se inician mediante los mandatos planificados deben completarse. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejos:

- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

Estilo de planificación

Especifica si se utilizan reglas de planificación clásicas o mejoradas.

Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que DAYOFWEEK=ANY). No se visualiza para las planificaciones de sintaxis mejoradas.

Día de la semana

Categoría principal de anotación: admin_info
Categoría secundaria de anotación: location
Asunto de anotación: codjo
Número de línea de anotación: 1
Datos de anotación: Toronto 5A24
Fecha/hora de creación: 2013-09-10, 10:15:50
Fecha/hora última actualización: 2013-09-10, 10:15:50
Última actualización por (administrador): CODJO

Categoría principal de anotación: admin_info
Categoría secundaria de anotación: location
Asunto de anotación: jane
Número de línea de anotación: 1
Datos de anotación: Raleigh GF85
Fecha/hora de creación: 2013-09-09, 14:29:40
Fecha/hora última actualización: 2013-09-09, 14:29:40
Última actualización por (administrador): JANE_W

Categoría principal de anotación: admin_info
Categoría secundaria de anotación: location
Asunto de anotación: jane
Número de línea de anotación: 2
Datos de anotación: Fuera de la oficina del 1-15 Nov.
Fecha/hora de creación: 2013-09-09, 14:30:05
Fecha/hora última actualización: 2013-10-31, 16:55:52
Última actualización por (administrador): JANE_W

Categoría principal de anotación: admin_info
Categoría secundaria de anotación: location
Asunto de anotación: montse
Número de línea de anotación: 1
Datos de anotación: Barcelona B19
Fecha/hora de creación: 2013-09-10, 04:34:37
Fecha/hora última actualización: 2013-09-10, 04:34:37
Última actualización por (administrador): MONTSERRAT

Descripciones de los campos

Datos de registro

Los datos que se almacenan en la entrada del área de registro.

Fecha/hora de creación

Fecha y hora en la que se creó la entrada de registro.

Fecha/hora última actualización

Fecha y hora en la que se actualizó por última vez la entrada de registro.

Última actualización por (administrador)

El administrador que actualizó por última vez la entrada de registro.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SCRATCHPADENTRY

Mandato	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

QUERY SCRIPT (Consultar scripts IBM Spectrum Protect)

Utilice este mandato para visualizar la información sobre scripts.

Puede utilizar este mandato con el mandato DEFINE SCRIPT para crear un nuevo script utilizando el contenido de otro script.

Clase de privilegio

La clase de privilegios necesaria para este mandato depende de si se ha especificado el parámetro Outputfile en el mandato.

- Si no se especifica el parámetro Outputfile, cualquier administrador puede emitir este mandato.
- Si se ha especificado el parámetro Outputfile y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES, el administrador debe tener privilegio de sistema.
- Si se ha especificado el parámetro Outputfile y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de políticas, de almacenamiento o de sistema.

Sintaxis

```

      .-*-----
>>-Query SCRipt--+-+-----+----->
      '-nombre_script-'

.-FORMAT-----Standard-----
>--+-+-----+-----<
  '-FORMAT-----+-Standard-----+'
      +-Detailed-----+
      +-Lines-----+
      '-Raw-----+'
      '-Outputfile-----nombre_archivo-'

```

Parámetros

nombre_script

Especifica el nombre del script cuya información se va a visualizar. Puede incluir un carácter comodín para especificar este nombre.

Importante: Si no especifica un script, la consulta visualizará la información sobre todos los scripts. El tiempo utilizado para procesar este mandato y la cantidad de información visualizada pueden ser considerables.

Format

Especifica el formato de salida para visualizar la información de script. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que sólo se visualizarán el nombre del script y la descripción.

Detailed

Especifica que se visualiza información detallada sobre el script. Esta información incluye los mandatos del script y los números de línea, la fecha de la última actualización y el administrador que ha realizado las actualizaciones.

Lines

Especifica que se visualizan el nombre del script, el número de línea de los mandatos, las líneas de comentarios y los mandatos que hay en el script.

Raw

Especifica que los mandatos incluidos en el script se graban en un archivo indicado con el parámetro Outputfile. Este formato es un modo de dirigir la salida de un script a un archivo para poder copiarlo en otro script con el mandato DEFINE SCRIPT.

Si no se especifica ningún archivo de salida, el servidor de IBM Spectrum Protect enviará la salida de "query script" con "format=raw" a la consola.

Outputfile

Especifica el nombre del archivo al que se dirige la salida si se especifica FORMAT=Raw. El archivo que especifique debe estar en el servidor que ejecuta este mandato. Si existe el archivo, la salida de la consulta se agrega al final del archivo.

Ejemplo: obtener una lista de las descripciones de los scripts

Visualizar la información estándar relativa a scripts.

```
query script *
```

Nombre	Descripción
QCOLS	Visualiza columnas para una tabla SQL especificada
QSAMPLE	Consulta SQL de ejemplo
EXAMPLE	Copia de seguridad de las agrupaciones de almacenamiento y base de datos cuando no hay sesiones

Ejemplo: visualizar el contenido de un script con números de líneas

Visualizar la información de líneas del script denominado Q_AUTHORITY.

```
query script q_authority format=lines
```

```
Nombre      Núm.  Mandato
-----
Q_AUTHORITY 1      /* -----*/
5          /* Nombre script: Q_AUTHORITY */
10         /* Descripción: Visualizar administradores */
15         /* con autorización para emitir */
20         /* mandatos que requieran un */
25         /* privilegio específico. */
30         /* Parámetro 1: nombre privilegio - formato */
35         /* x_priv - EX. policy_priv */
40         /* Ejemplo: run q_authority storage_priv */
45         /* -----*/
50         select admin_name from admins where -
55         upper(system_priv) <> 'NO' or -
60         upper($1) <> 'NO'
```

Ejemplo: crear un script a partir de un script existente

Consultar el script ENGDEV y dirigir la salida a un archivo denominado MY.SCRIPT.

```
query script engdev format=raw outputfile=my.script
```

Ejemplo: visualizar información detallada acerca del script

Visualizar la información detallada sobre los scripts. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query script * format=detailed
```

```
Nombre: QCOLS
Número líneas: DESCRIPTION
Mandato: Visualizar columnas para
una tabla
SQL especificada
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 12/02/1997 16:05:29

Nombre: QCOLS
Número líneas: 1
Mandato: select colname from
columns where
tabname='$1'
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 12/02/1997 16:05:29
```

Descripciones de los campos

Nombre

El nombre del script.

Número de línea

El número de línea del script o la serie DESCRIPTION.

Mandato

El mandato incluido en el número de línea visualizado en el campo anterior.

Última actualización por (administrador)

El nombre del administrador que ha definido o ha actualizado más recientemente el script.

Fecha/hora de la última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente el script.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SCRIPT

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.

Mandato	Descripción
DELETE SCRIPT	Suprime el script o líneas individuales del script.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

Conceptos relacionados:

Scripts de servidor

QUERY SERVER (Consultar un servidor)

Utilice este mandato para visualizar información acerca de una definición de servidor.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-*-----*
>>-Query SERver--+-----+----->
      '-nombre_servidor-'

      .-Format----Standard-----
>--+-----+-----<<
      '-Format-----Standard-+-'
      '-Detailed-'

```

Parámetros

nombre_servidor

Especifica el nombre del servidor que se va a consultar. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todos los nombres de servidores.

Format

Especifica cómo se ha de visualizar la información. El parámetro es opcional. El valor predeterminado es STANDARD.

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: obtener una lista de todos los servidores

Visualizar información en el formato estándar relativa a todos los servidores. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query server *
```

Nombre servidor	Método com.	Dirección alto nivel	Dirección bajo nivel	Días desde últ. acceso	Contras. servidor asignada	Contras. volumen virtual asignada	Permitir sustit.
SERVER_A	TCPIP	9.115.35.6	1501	11	Yes	No	No
SERVER_B	TCPIP	9.115.45.24	1500	<1	Yes	No	No
ASTRO	TCPIP	9.115.32.21	1500	24	Yes	No	No

Ejemplo: visualizar información detallada acerca de un servidor específico

Desde un servidor gestionado, visualizar información detallada sobre el SERVER_A. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query server server_a format=detailed
```

```

Nombre servidor: SERVER_A
Método comunicaciones: TCPIP
Método de transferencia: TCPIP
Dirección alto nivel: 9.115.4.15
Dirección bajo nivel: 1500
Descripción:
Permitir sustitución: No
Nombre nodo:
Fecha/hora último acceso : 09.07.2013 09:00:00
Días desde último acceso: <1
Compresión: Elección del cliente
¿Supresión copias archivadas?: No
URL:
Fecha/hora registro: 07/08/2013 09:15:09
Registrado por administrador: $$CONFIG_MANAGER$$
Bytes recibidos última sesión: 362
Bytes enviados última sesión: 507
Duración de última sesión: 0,00
Porcentaje de esperas desocupado
última sesión: 0,00
Porcentaje de Método comunicaciones
última sesión: 0.00
Porcentaje de esperas medio
última sesión: 0,00
Período gracia supresión: 5
Perfil de gestión:
Contraseña servidor asignada: Si
Fecha/hora asignación contraseña servidor: 07/08/2013 09:15:09
Días desde establecimiento de contraseña de servidor: 1
Número inicios sesión no válidos servidor: 0
Contraseña volumen virtual asignada: No
Fecha/hora asignación volúmenes volumen virtual:(?)
Días desde asignación contraseña volumen
virtual:(?)
Número inicios sesión no válidos nodo
volumen virtual: 0
Protocolo de validación: No
Versión: 7
Release: 1
Nivel: 0.0
Rol(es): Réplica
SSL: No
Session Security: Strict
Transport Method: TLS 1.2

```

Descripciones de los campos

Nombre del servidor

El nombre del servidor.

Método comunicaciones

El método de comunicación que se utiliza para conectarse al servidor.

Método de transferencia

El método que se utiliza para la transferencia de datos de servidor a servidor.

Dirección alto nivel

La dirección IP (con formato de puntos) del servidor.

Dirección bajo nivel

El número de puerto del servidor.

Descripción

La descripción del servidor.

Permitir sustitución

Especifica si una definición de servidor en un servidor gestionado puede sustituirse por una definición de un gestor de configuración.

Nombre del nodo

El nombre del nodo de cliente.

Fecha/hora último acceso

La última fecha y hora en que el nodo de cliente ha accedido al servidor.

Días desde último acceso

El número de días transcurridos desde que el nodo cliente accedió al servidor.

Compresión

El tipo de compresión que IBM Spectrum Protect completa en los archivos de cliente.

¿Supresión copias archivadas?

Especifica si el nodo de cliente puede suprimir sus propias copias archivadas. Un valor de (?) indica que este campo no se ha establecido y no se aplica a esta definición.

URL

El URL utilizado para acceder a este servidor desde una interfaz basada en un navegador web.

Fecha/hora registro

La fecha y la hora en que se ha inscrito el nodo cliente.

Registrado por administrador

El nombre del administrador que ha inscrito el nodo cliente.

Bytes recibidos última sesión

El número de bytes que ha recibido el servidor durante la última sesión del nodo de cliente.

Bytes enviados última sesión

El número de bytes enviados al nodo de cliente.

Duración última sesión

El tiempo que ha durado la última sesión del nodo de cliente, en segundos.

Porcentaje de esperas desocupado última sesión

El porcentaje del tiempo total de la sesión durante la cual el cliente no ha realizado ninguna función.

Porcentaje de Método comunicaciones última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando una respuesta del servidor.

Porcentaje de esperas soporte última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando que se montara un volumen extraíble.

Periodo de gracia de supresión

El número de días que un objeto permanece en el servidor de destino después de que se haya marcado para suprimirlo.

Perfil de gestión

El perfil del que el servidor gestionado ha obtenido la definición de este servidor.

Contraseña servidor establecida

Especifica si la contraseña del servidor se ha establecido.

Fecha/hora de establecimiento de contraseña de servidor

Especifica cuándo se ha establecido la contraseña del servidor.

Días desde asignación de contraseña de servidor

Especifica el número de días transcurridos desde que se ha asignado la contraseña del servidor.

Número inicios sesión no válidos para el servidor

El número máximo de intentos de inicio de sesión no válidos que el servidor puede aceptar.

Contraseña de volumen virtual establecida

Especifica si la contraseña que se utiliza para iniciar la sesión en el servidor de destino se ha establecido.

Fecha/hora de establecimiento de contraseña de volumen virtual

Especifica cuándo se ha establecido la contraseña del soporte de volumen virtual.

Días desde establecimiento de contraseña de volumen virtual

Especifica el número de días transcurridos desde que se ha asignado la contraseña del soporte de volúmenes virtuales.

Número de inicios de sesión no válidos para nodo de volumen virtual

El número máximo de intentos de inicio de sesión no válidos que se aceptan en el servidor de destino.

Protocolo de validación (en desuso)

Especifica si el agente de almacenamiento tiene activada la función de validación de datos. Este campo está en desuso.

Versión

La versión de software del servidor de IBM Spectrum Protect.

Release

El release del software del servidor de IBM Spectrum Protect.

Nivel

El nivel de software del servidor de IBM Spectrum Protect.

Rol(es)

El rol del servidor. Por ejemplo, uno de los roles para los que se utiliza el servidor es la duplicación.

SSL

Especifica si se utiliza la comunicación de la capa de sockets seguros (SSL).

Seguridad de sesión

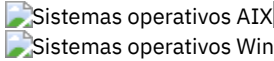
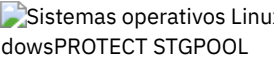
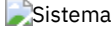
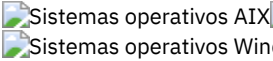
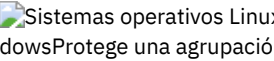

Especifica el nivel de seguridad de sesión que se impone para el servidor. Los valores pueden ser STRICT o TRANSITIONAL.

Método de transporte

Especifica el método de transporte que se ha utilizado la última vez para el servidor especificado. Los valores pueden ser TLS 1.2, TLS 1.1 o NONE. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SERVER

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PROTECT STGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE SERVER	Actualiza la información sobre un servidor.

QUERY SERVERGROUP (Consultar un grupo de servidores)

Utilice este mandato para visualizar información sobre grupos de servidores y miembros de grupos.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-QUERY SERVERGroup--*-----<
                        |-----|
                        '-nombre_grupo-'
```

Parámetros

nombre_grupo

Especifica el grupo de servidores que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre.

Ejemplo: obtener una lista de grupos de servidores

Desde un servidor gestionado, consultar todos los grupos de servidores. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query servergroup *
```

Grupo serv.	Miembros	Descripción	Perfil gestión
ADMIN_GROUP	SERVER_A SERVER_B SERVER_C SERVER_D	Headquarters	ADMIN_INFO

Descripciones de los campos

Grupo de servidores

El nombre del grupo de servidores.

Miembros

Los miembros del grupo.

Descripción

La descripción del grupo de servidores.

Perfil de gestión

El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de los grupos de servidores.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SERVERGROUP

Mandato	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

QUERY SESSION (Consultar sesiones de cliente)

Utilice este mandato para visualizar información sobre sesiones administrativas, de nodo y de servidor.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query SEssion----->
      '-númsesión-'

>----->
      '-MINTIMethreshold---minutes-'

>----->
      '-MAXTHRoughput---kilobytes_por_segundo-'

      .-Format---Standard-. .-Type---*-----
>----->
      '-Format---Standard+-' '-Type---+Admin--+'
          '-Detailed-'          +-Node---+
                                '-Server-'

      .-CLIENTName---*-----
>-----<
      '-CLIENTName---nombre_cliente---
```

Parámetros

númsesión

Especifica el número de la sesión de nodo de cliente o de administración que se consulta. Este parámetro es opcional. Si no especifica un valor para este parámetro, se visualizarán todas las sesiones.

MINTIMethreshold

Especifica visualizar las sesiones que han tenido como mínimo este número de minutos transcurridos desde la hora en que el cliente ha enviado datos al servidor para su almacenamiento. Este parámetro es opcional. El número mínimo de minutos es 1. El número máximo de minutos es 99999999.

MAXTHROUGHput

Especifica visualizar sesiones que están transfiriendo datos a una velocidad inferior a este número de kilobytes por segundo. Este parámetro es opcional. El número mínimo de kilobytes por segundo es de 0. El número máximo de kilobytes por segundo es de 99999999.

Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualizará información parcial para la sesión.

Detailed

Especifica que se visualizará información completa para la sesión.

Type

Especifica el tipo de sesiones a incluir en el resultado de la consulta. Si no especifica un valor para este parámetro, se consultarán todos los tipos de sesión. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Admin

Especifica que se visualizan las sesiones administrativas.

Node

Especifica que se visualizan las sesiones de nodo.

Server

Especifica que se visualizan las sesiones de servidor.

CLIENTName

Especifica el nombre de un administrador, nodo de cliente o servidor a consultar. Puede especificar uno o más nombres. También puede especificar grupos de nodos y nodos proxy. Si especifica varios nombres, sepárelos mediante comas, no utilice espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos. El parámetro es opcional.

Durante la replicación de nodos, el nombre de cliente del servidor de destino se visualiza como *nombre_nodo* (*nombre_servidor*), donde *nombre_nodo* es el nodo cuyos datos se están replicando y *nombre_servidor* es el nombre del servidor de origen. Puede especificar el nombre del nodo o bien el nombre del servidor en el parámetro CLIENTName para visualizar las sesiones de replicación.

Ejemplo: obtener una lista de las sesiones de nodo cliente activas

Visualizar información acerca de todas las sesiones de nodo cliente y de administración que están comunicándose con el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query session
```

Núm. sesión	Método comun.	Estado sesión	Tiempo espera	Bytes env.	Bytes rec.	Tipo sesión	Plataf.	Nombre cliente
4	TCP/IP	Run	0 S	1.4 K	162	Admin	WinNT	ADMIN

Ejemplo: visualizar información detallada acerca de las sesiones de nodo cliente activas

Visualizar información detallada acerca de todas las sesiones de nodo de cliente y de administración que están comunicándose con el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query session format=detailed
```

```
Número sesión: 4
Método comunicaciones: Tcp/Ip
Estado sesión: Run
Tiempo de espera: 0 S
Bytes enviados: 1,4 K
Bytes recibidos: 162
Tipo de sesión: Admin
Plataforma: WinNT
Nombre de cliente: ADMIN
```

Estado del acceso al soporte:
Nombre usuario:
Fecha/hora primer envío datos:
Proxy mediante agente de almacenamiento:
Acciones:
Modalidad de migración tras error: No

Descripciones de los campos

Número sesión

Especifica un número de identificación de sesión exclusivo que asigna el servidor.

Método comunicaciones

Especifica el método que está utilizando el cliente para comunicarse con el servidor.

Estado sesión

Especifica el estado actual de las comunicaciones del servidor. Son posibles los siguientes estados:

END

La sesión está finalizando (se liberan los recursos de sesión).

IDLEW

En espera de la siguiente petición del cliente (la sesión está en estado de desocupación).

Espera medio

La sesión está a la espera de acceso a un volumen de acceso secuencial.

RECVW

A la espera de recibir un mensaje del cliente.

RUN

El servidor está ejecutando una petición del cliente (y no a la espera de enviar datos).

SENDW

El servidor está a la espera de enviar datos al cliente (a la espera de que los datos que ya se han enviado se entreguen al nodo de cliente).

SSLiW

La sesión está esperando a que finalice la inicialización de la capa de sockets seguros (SSL).

START

Se está iniciando la sesión (la autenticación está en proceso).

Tiempo espera

Especifica la cantidad de tiempo (segundos, minutos u horas) en que el servidor ha estado en el estado actual mostrado.

Bytes enviados

Especifica el número de bytes de datos enviados al nodo de cliente desde que se ha iniciado la sesión.

Bytes rec.

Especifica el número de bytes de datos recibidos del nodo de cliente desde que se ha iniciado la sesión.

Tipo

Especifica el tipo de sesión en curso: ADMIN para una sesión de administración, NODE para una sesión de nodo de cliente o SERVER. SERVER especifica que el servidor inicia una sesión e inicia operaciones de servidor como la configuración central, compartimiento de biblioteca y sesiones de agente de almacenamiento.

Plataforma

Especifica el tipo de sistema operativo asociado con el cliente.

Nombre cliente

Especifica el nombre del nodo cliente o el administrador.

Para las sesiones de réplica de nodo, el nombre del cliente se actualiza a *nombre_nodo* (*nombre_servidor*) en el servidor de destino tras iniciar la transferencia de datos.

Estado de acceso al medio

Especifica el tipo de estado de espera del medio. Cuando una sesión se encuentra en un estado de espera de medios, este campo muestra una lista de todos los puntos de montaje y los volúmenes secuenciales de la sesión. La lista de puntos de montaje especifica la clase de dispositivo y la agrupación de almacenamiento asociada. La lista de volúmenes especifica los volúmenes de agrupación de almacenamiento primaria además de los volúmenes de agrupación de almacenamiento de copia y de agrupación de datos activos con su agrupación de almacenamiento asignada.

El servidor permite a varias sesiones la lectura y a una sesión la grabación en un volumen simultáneamente en una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA. Como resultado, un volumen en una agrupación de almacenamiento con el tipo de dispositivo FILE o CENTERA puede aparecer como el volumen actual en más de una sesión.

Proxy mediante agente de almacenamiento

Especifica el agente de almacenamiento que es el proxy de movimiento de datos fuera de la LAN para el nodo.

Nombre usuario

Especifica el identificador de usuario del nodo en un sistema de multiusuario, que se conecta con el servidor cuando no es el mismo usuario del sistema que se ha conectado originalmente con el servidor.

Fecha/hora primer envío datos

Especifica la fecha y hora en que el cliente ha enviado por primera vez datos al servidor para su almacenamiento.

Acciones

Muestra una lista de acciones que se realizan durante la sesión. Una acción se lista una sola vez, aunque se produzca varias veces durante una sesión. Son posibles las acciones siguientes:

BkIns

Se han almacenado uno o más objetos de copia de seguridad en el servidor. La operación puede haberse basado en una copia de seguridad incremental o selectiva.

BkUpd

Se han actualizado uno o más atributos para un objeto de copia de seguridad que está almacenada en el servidor.

BkDel

Se han eliminado uno o más objetos de copia de seguridad en el servidor.

BkRebind

Uno o más objetos de copia de seguridad almacenados en el servidor están vinculados a una clase de gestión diferente.

NoQueryRestore

Una operación de restauración sin consulta se ha iniciado desde el cliente para restaurar los archivos de copia de seguridad del servidor al sistema cliente.

ArIns

Se han almacenado uno o más objetos de archivado en el servidor.

ObjRtrv

Se han recuperado uno o más archivos del servidor. Puede servir para recuperar archivos de copia archivada, o para restaurar datos de copia de seguridad (excepto para datos de copia de seguridad procedentes de una operación de restauración no solicitada).

MigIns

Uno o más archivos se han migrado y almacenado en el servidor mediante IBM Spectrum Protect for Space Management (cliente HSM).

MigDel

Se han suprimido uno o más archivos gestionados por espacio que estaban almacenados en el servidor.

MigRebind

Uno o más archivos gestionados por espacio que estaban almacenados en el servidor se han vinculado a una clase de gestión distinta.

MigRecall

Se han recuperado uno o más archivos gestionados por espacio almacenados en el servidor.

MigUpd

Se han actualizado los atributos de uno o más archivos gestionados por espacio que estaban almacenados en el servidor.

FSAdd

El nodo de cliente ha agregado uno o más espacios de archivo nuevos al almacenamiento del servidor.

FSUpd

El nodo de cliente ha actualizado los atributos para uno o más espacios de archivo que están definidos en el servidor.

DefAuth

El nodo de cliente ha procesado un mandato SET ACCESS, lo que ha hecho que se agregara una regla de autorización para el acceso a los datos del nodo de cliente.

Modalidad de migración tras error

Especifica si la sesión de cliente se ha iniciado en modalidad de recuperación de errores. Son posibles los siguientes valores:

Fuerza

Se especifica FORCEFAILOVER en el cliente y se fuerza la modalidad de migración tras error de sesión.

Sí

La sesión de cliente se ha iniciado en modalidad de recuperación de errores.

No

La sesión de cliente no se ha iniciado en modalidad de recuperación de errores.

Mandatos relacionados

Tabla 1. Mandato relacionado con QUERY SESSION

Mandato	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.

QUERY SHREDSTATUS (Consultar estado de destrucción)

Utilice este mandato para visualizar información acerca de los datos en espera de ser destruidos.

Clase de privilegio

Para emitir este mandato, debe tener privilegios de administrador.

Sintaxis

```
>>-QUERY SHREDstatus--+-Format--Standard-----><
                          '-Format--Standard--'
                          '-Detailed-'
```

Parámetros

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial. Este es el valor predeterminado.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información de destrucción de resumen

Muestra información parcial sobre la destrucción de datos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query shredstatus

Destrucción Objetos
activa      para
           destruir
-----
NO         4
```

Ejemplo: visualizar información de destrucción detallada

Muestra información detallada sobre la destrucción de datos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query shredstatus format=detailed

Destrucción Objetos Espacio Datos restantes
Active  Awaiting Space  To Shred
        Shred   (MB)   (MB)
-----
NO      4       182    364
```

Descripciones de los campos

Destrucción activa

Indica si el servidor está destruyendo datos de forma activa en este momento.

Objetos para destruir

El número de objetos en espera de destruirse.

Espacio ocupado (MB)

La cantidad de espacio de almacenamiento del servidor ocupado por los objetos que actualmente están en espera de destruirse, en megabytes. Es la cantidad de espacio que pasará a estar disponible cuando se destruyan los objetos.

Datos restantes para destruir (MB)

La cantidad de datos que todavía se tienen que destruir.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SHREDSTATUS

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
SETOPT	Actualiza una opción del servidor sin parar y reiniciar el servidor.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

QUERY SPACETRIGGER (Consultar los desencadenantes de espacio)

Utilice este mandato para visualizar los valores de los desencadenantes de espacio de agrupación de almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query SPACETrigger--STG----->
>--+-----+----->
  '-STGPOOL----agrupación_almacenamiento-'
  .-Format----Standard----.
>--+-----+-----<<
  '-Format---+Standard+-'
      '-Detailed-'
```

Parámetros

STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

STGPOOL

Especifica una o varias agrupaciones de almacenamiento (mediante un comodín) para las que se visualizará información de desencadenantes de agrupación. Si STG está especificado, pero STGPOOL no, se visualiza el desencadenante de espacio predeterminado de la agrupación de almacenamiento, si lo hay.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: visualizar información detallada acerca de los valores de un desencadenante de espacio de agrupación de almacenamiento

Emita este mandato:

```
query spacetrigger stg stgpool=archivepool format=detailed
```

Sistemas operativos AIX

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: /usr/tivoli/tsm/
                             server/filevol/
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

Sistemas operativos Linux

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: /opt/tivoli/tsm/server
                             /filevol/
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

Sistemas operativos Windows

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: c:\program files\tivoli
                             \filevol\
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

Descripciones de los campos

STGPOOL Full Percentage

El porcentaje de utilización de desencadenante en que IBM Spectrum Protect asigna más espacio para la agrupación de almacenamiento.

STGPOOL Expansion Percentage

Porcentaje de espacio según el cual se amplía la agrupación de almacenamiento.

Prefijo de ampliación STGPOOL

El prefijo asociado al desencadenante de espacio.

STGPOOL

Nombre de la agrupación de almacenamiento asociado a la consulta.

Última actualización por (administrador)

Administrador que actualizó por última vez el desencadenante de espacio de la agrupación de almacenamiento.

Fecha/hora de la última actualización

Fecha y hora de la última actualización por parte del administrador del desencadenante de espacio de la agrupación de almacenamiento.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SPACETRIGGER

Mandato	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

QUERY STATUS (Consultar parámetros del sistema)

Utilice el mandato QUERY STATUS para visualizar información sobre los parámetros del sistema.

Utilice este mandato para las tareas siguientes:

- Para visualizar el nivel de servicio del servidor
- Para visualizar información acerca de los parámetros generales del servidor, como por ejemplo los definidos mediante los mandatos SET.
- Para solicitar información acerca de las sesiones cliente, como por ejemplo la disponibilidad del servidor, la autenticación de contraseñas, los valores de contabilidad, o el período de retención de la información retenida en el registro de actividad.
- Para visualizar información acerca del planificador central, como por ejemplo la modalidad de planificación central del servidor.
- Para visualizar el número máximo de intentos repetidos que se permiten después de un intento anómalo de ejecutar un mandato planificado.
- Para visualizar si se pueden hacer copias de seguridad de los subarchivos en este servidor, como indica el mandato SET SUBFILE
- Para visualizar información sobre un servidor de réplica de destino
- Para mostrar información de licencias

Consejo: Para visualizar información sobre un servidor de réplica de destino, debe emitir el mandato desde el servidor de réplica de destino.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query STatus-----<<
```


Parámetros

Ninguno.

Ejemplo: consultar el estado de un gestor de configuración

Visualizar información general acerca de los parámetros del servidor. El mandato se ejecuta desde un gestor de configuración. Para ver una descripción de los campos mostrados, consulte Descripciones de los campos.

```
query status
```

 Sistemas operativos AIX

```
Nombre de servidor: SETSHOT
Nombre host servidor o dirección IP: setshot
Número puerto TCP/IP servidor: 1500
Autenticación: Activada
Contraseña servidor asignada: Sí
Fecha/hora de instalación de servidor: 2016-07-08, 09:45:53
Fecha/hora de reinicio de servidor: 2016-10-10, 05:38:49
Autenticación: Desactivada
Período caducidad contraseña: 9.999 día(s)
Límite conexiones no válidas: 0
Longitud mínima contraseña: 0
Inscripción: Cerrada
Copia de seguridad de subarchivos: Cliente
Disponibilidad: Activada
Sesiones de entrada desactivadas:
Sesiones de salida desactivadas:
Contabilidad: Desactivada
Período retención registro actividades: 30 día(s)
Número de registros de registro de actividad: 222919
Tamaño del registro de actividad: 6 M
Período retención resumen actividades: 30 día(s)
Período auditoría licencia: 30 día(s)
Última auditoría de licencia: 2016-10-21, 07:40:20
Cumplimiento licencia servidor: Válido
Planificador central: Activo
Sesiones máximas: 300
Sesiones planificadas máximas: 75
Período retención registros eventos: 14 día(s)
Duración acción cliente: 5 día(s)
```

Porcentaje aleatorización planificaciones: 25
 Período consulta planificaciones: Opción cliente
 Máximo reintentos mandatos: Opción cliente
 Período reintento: Opción cliente
 Nivel de verificación de deduplicación del lado del cliente: 0%
 Modalidades planificación: Cualquiera
 Receptores activos: CONSOLE ACTLOG
 Gestor configuración: Desactivado
 Intervalo renovación: 60
 Fecha/hora última renovación:
 Envío de mensajes de contexto: Activado
 Período retención de carga tabla contenido (TOC): 120 Minuto(s)
 ID exclusivo global de máquina: d4.cg.f6.ae.04.6e.11.e3.80.1f.00.21.5e.18.df.01
 Protección retención copias archivadas: desactivada
 Directorios de base de datos: /TSMserver/DB1,/TSMserver/DB2
 Espacio total de sistema de archivos (MB): 222.720,00
 Espacio utilizado en el sistema de archivos (MB): 47.780,74
 Espacio libre disponible (MB): 174.939,26
 Nivel de cifrado: AES
 Intervalo de renovación de información de CPU de cliente: 180
 Réplica de salida: activado
 Servidor de réplica de destino: POWER
 Regla de réplica predeterminada de archivado: ALL_DATA
 Regla de réplica predeterminada de copia de seguridad: ALL_DATA
 Regla de réplica predeterminada para gestión de espacio: ALL_DATA
 Período de retención de registros de réplica: 30 día(s)
 Usuario LDAP:
 Contraseña LDAP establecida: No
 Autenticación predeterminada: Local
 Dirección de alto nivel de migración tras error:
 Retención de anotación: 365 día(s)
 Recuperación de duplicación de archivos dañados: activado
 Ocupación SUR (TB): 5.66
 Fecha/hora de ocupación SUR: 2016-10-10, 05:39:33
 Capacidad inicial (MB): 226.331
 Recuento de cliente inicial: 6
 Fecha de capacidad inicial: 2016-10-13, 09:20:02
 Oferta de producto: IBM Spectrum Protect

Sistemas operativos Linux

 Nombre de servidor: GOBI
 Nombre host servidor o dirección IP:
 Número puerto TCP/IP servidor: 1500
 Autenticación: Activada
 Contraseña servidor asignada: Si
 Fecha/hora de instalación de servidor: 2016-07-08, 11:29:03
 Fecha/hora de reinicio de servidor: 2016-11-10, 14:25:03
 Autenticación: Activada
 Período caducidad contraseña: 90 día(s)
 Límite conexiones no válidas: 0
 Longitud mínima contraseña: 0
 Inscripción: Cerrada
 Copia de seguridad de subarchivos: No
 Disponibilidad: Activada
 Sesiones de entrada desactivadas:
 Sesiones de salida desactivadas:
 Contabilidad: Desactivada
 Período retención registro actividades: 30 día(s)
 Número de registros de registro de actividad: 21346
 Tamaño del registro de actividad: <1 M
 Período retención resumen actividades: 30 día(s)
 Período auditoría licencia: 30 día(s)
 Última auditoría de licencia: 2016-10-21, 23:27:23
 Cumplimiento licencia servidor: Válido
 Planificador central: Activo
 Sesiones máximas: 500
 Sesiones planificadas máximas: 250
 Período retención registros eventos: 14 día(s)
 Duración acción cliente: 5 día(s)
 Porcentaje aleatorización planificaciones: 25
 Período consulta planificaciones: Opción cliente
 Máximo reintentos mandatos: Opción cliente
 Período reintento: Opción cliente
 Nivel de verificación de deduplicación del lado del cliente: 0%
 Modalidades planificación: Cualquiera
 Receptores activos: CONSOLE ACTLOG

Gestor configuración: Desactivado
 Intervalo renovación: 60
 Fecha/hora última renovación:
 Envío mensajes contexto: Desactivado
 Período retención de carga tabla contenido (TOC): 120 Minuto(s)
 ID exclusivo global de máquina: fc.e7.be.58.4a.a7.11.e0.8a.c8.e4.1f.13.34.11.e0
 Protección retención copias archivadas: desactivada
 Dir. base datos:
 /TSMdbspace1/gpcinst1,/TSMdbspace2/gpcinst1,/TSMdbspace3/gpcinst1
 Espacio total de sistema de archivos (MB): 302.379,84
 Espacio utilizado en sistema de archivos (MB): 106.793,65
 Espacio libre disponible (MB): 195.586,20
 Nivel de cifrado: AES
 Intervalo de renovación de información de CPU de cliente: 180
 Réplica de salida: activado
 Servidor de réplica de destino:
 Regla de réplica predeterminada de archivado: ALL_DATA
 Regla de réplica predeterminada de copia de seguridad: ALL_DATA
 Regla de réplica predeterminada para gestión de espacio: ALL_DATA
 Período de retención de registros de réplica: 30 día(s)
 Usuario LDAP:
 Contraseña LDAP establecida: No
 Autenticación predeterminada: Local
 Dirección de alto nivel de migración tras error:
 Retención de anotación: 365 día(s)
 Recuperación de duplicación de archivos dañados: desactivado
 Ocupación SUR (TB): 0,00
 Fecha/hora ocupación SUR: 2016-10-10, 14:25:35
 Capacidad inicial (MB): 226.331
 Recuento de cliente inicial: 6
 Fecha de capacidad inicial: 2016-10-13, 09:20:02
 Oferta de producto: IBM Spectrum Protect

Sistemas operativos Windows

Nombre de servidor: EXCELSIOR
 Nombre host servidor o dirección IP: excelsior.storage.
 newyork.example.com
 Número puerto TCP/IP servidor: 1500
 Autenticación: Activada
 Contraseña servidor asignada: Sí
 Fecha/hora de instalación de servidor: 2016-07-08, 18:02:50
 Fecha/hora de reinicio de servidor: 2016-11-10, 11:48:32
 Autenticación: Activada
 Período caducidad contraseña: 90 día(s)
 Límite conexiones no válidas: 0
 Longitud mínima contraseña: 0
 Inscripción: Cerrada
 Copia de seguridad de subarchivos: No
 Disponibilidad: Activada
 Sesiones de entrada desactivadas:
 Sesiones de salida desactivadas:
 Contabilidad: Activada
 Período retención registro actividades: 30 día(s)
 Número de registros de registro de actividad: 1346376
 Tamaño del registro de actividad: 37 M
 Período retención resumen actividades: 30 día(s)
 Período auditoría licencia: 30 día(s)
 Última auditoría de licencia: 2016-10-21, 17:05:16
 Cumplimiento licencia servidor: Válido
 Planificador central: Activo
 Sesiones máximas: 25
 Sesiones planificadas máximas: 12
 Período retención registros eventos: 14 día(s)
 Duración acción cliente: 5 día(s)
 Porcentaje aleatorización planificaciones: 25
 Período consulta planificaciones: Opción cliente
 Máximo reintentos mandatos: Opción cliente
 Período reintento: Opción cliente
 Nivel de verificación de deduplicación del lado del cliente: 0%
 Modalidades planificación: Cualquiera
 Receptores activos: CONSOLE ACTLOG
 NTEVENTLOG
 Gestor configuración: Desactivado
 Intervalo renovación: 60
 Fecha/hora última renovación:

```

Envío mensajes contexto: Desactivado
Período retención de carga tabla contenido (TOC): 120 Minuto(s)
  ID exclusivo global de máquina: e9.3e.fl.70.ff.c5.11.e2.
    a5.67.5c.f3.fc.0c.5e.60
  Protección retención copias archivadas: desactivada
  Directorios de base de datos: e:\Server1\TSMDBdir
Espacio total de sistema de archivos (MB): 102.270,00
Espacio utilizado en sistema de archivos (MB): 22.032,79
Espacio libre disponible (MB): 80.237,20
  Nivel de cifrado: AES
Intervalo de renovación de información de CPU de cliente: 180
  Réplica de salida: activado
  Servidor de réplica de destino: EXPLORER
Regla de réplica predeterminada de archivado: ALL_DATA
Regla de réplica predeterminada de copia de seguridad: ALL_DATA
Regla de réplica predeterminada para gestión de espacio: ALL_DATA
  Período de retención de registros de réplica: 30 día(s)
    Usuario LDAP: cn=excelsior_ldapadmin,ou=excelsior,
      ou=John Doe,dc=tsmadldap,dc=storage,
      dc=newyork, dc=example,dc=com
  Contraseña LDAP establecida: Yes
  Autenticación predeterminada: LDAP
Dirección de alto nivel de migración tras error:
  Retención de anotación: 365 día(s)
Recuperación de duplicación de archivos dañados: activado
  Ocupación SUR (TB): 8,98
  Fecha/hora de ocupación SUR: 2016-10-10, 11:49:27
  Capacidad inicial (MB): 226.331
  Recuento de cliente inicial: 6

```

 Sistemas operativos Windows

```

Fecha de capacidad inicial: 2016-10-13, 09:20:02
Oferta de producto: IBM Spectrum Protect

```

Descripciones de los campos

- Nombre del servidor
 - Especifica el nombre del servidor.
- Nombre del host del servidor o dirección IP
 - Especifica la dirección TCP/IP del servidor.
- Número de puerto TCP/IP del servidor
 - Especifica la dirección del puerto del servidor.
- Crossdefine
 - Especifica si otro servidor que ejecuta el mandato DEFINE SERVER se define automáticamente a sí mismo en este servidor.
 - Consulte el mandato SET CROSSDEFINE.
- Contraseña servidor establecida
 - Especifica si se ha asignado la contraseña para el servidor.
- Fecha/hora instalación servidor
 - Especifica la fecha y hora en que se ha instalado el servidor.
- Fecha/hora reinicio servidor
 - Especifica la última fecha y hora en que se ha iniciado el servidor.
- Autenticación
 - Especifica si está activada o desactivada la autenticación del servidor.
- Período de caducidad de contraseña
 - Especifica el período, en días, después del cual caduca la contraseña del nodo cliente o del administrador.
- Límite de conexiones no válidas
 - Especifica el número de intentos de inicio de sesión permitidos antes de bloquear un nodo.
- Longitud mínima contraseña
 - Especifica el número de caracteres mínimo que debe tener la contraseña.
- Inscripción
 - Especifica si la modalidad de inscripción de nodos cliente es abierta o cerrada.
- Copia de seguridad de subarchivos
 - Especifica si se pueden hacer copias de seguridad de los subarchivos en este servidor, como indica el mandato SET SUBFILE.
- Disponibilidad
 - Especifica si el servidor está activado o desactivado.
- Sesiones de entrada inhabilitadas
 - Especifica los nombres de los servidores desde los que no están permitidas las comunicaciones de servidor a servidor. Para activar las sesiones de servidor de entrada, utilice el mandato ENABLE SESSIONS.
- Sesiones de salida inhabilitadas

Especifica los nombres de los servidores hacia los que no están permitidas las comunicaciones de servidor a servidor. Para activar las sesiones de servidor de salida, utilice el mandato ENABLE SESSIONS.

Contabilidad

Especifica si se genera un registro de contabilidad al final de cada sesión del nodo cliente.

Período de registro de actividades

Especifica el número de días en que se retiene la información de las anotaciones de actividades o el tamaño del registro.

Número de registros de anotaciones de actividades

Especifica el número de registros de anotaciones de actividades.

Tamaño del registro de actividades

Especifica el tamaño de los registros de anotaciones de actividades.

Período retención resumen actividades

Especifica el número de días en que se retiene la información de la tabla resumen de actividad de SQL.

Período auditoría licencia

Especifica el período, en días, después del cual el gestor de licencias realiza automáticamente una auditoría de la licencia de IBM Spectrum Protect. Se puede disponer de información de auditorías adicional mediante el mandato QUERY LICENSE.

Última auditoría licencia

Especifica la fecha y hora en que se ha producido la última auditoría de licencia. Se puede disponer de información de auditorías adicional mediante el mandato QUERY LICENSE.

Cumplimiento licencia servidor

Especifica si el servidor de ADSM cumple (Válido) o no (No válido) con los términos de la licencia. Utilice el mandato QUERY LICENSE para ver cuáles son los factores que hacen que el servidor no cumpla los términos de la licencia.

Planificador central

Especifica si está ejecutándose la planificación central (activo o cancelado).

Máximo de sesiones

Especifica el número máximo de sesiones cliente/servidor.

Máximo de sesiones planificadas

Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.

Período de retención de registros de eventos

Especifica el número de días en que se retienen los registros de eventos del planificador central.

Duración acción de cliente

Especifica la duración del período durante el que el cliente procesa la planificación definida con el mandato DEFINE CLIENTACTION.

Porcentaje de aleatorización de planificaciones

Especifica la cantidad de margen de puesta en marcha que se utiliza para ejecutar los eventos planificados en modalidad de sondeo de cliente.

Período de consulta de planificaciones

Especifica la frecuencia con la que los clientes sondean el servidor para obtener el trabajo planificado, en modalidad de sondeo de cliente. Si el valor de este campo es Opción cliente, la frecuencia de sondeo la determina el nodo cliente.

Máximo reintentos mandatos

Especifica el número máximo de veces que un planificador del cliente intenta ejecutar un mandato planificado después de un intento fallido. Si el valor de este campo es Opción cliente, el número máximo lo determina el nodo de cliente.

Período de reintento

Especifica el número de minutos entre intentos fallidos de un planificador del cliente de contactar con el servidor o de ejecutar un mandato planificado. Si el valor de este campo es Opción cliente, el número de minutos lo determina el nodo de cliente.

Nivel de verificación de deduplicación del lado del cliente

Especifica un porcentaje de extensiones que debe verificar el servidor de IBM Spectrum Protect. Las extensiones se crean durante la eliminación de duplicados de datos del lado del cliente.

Modalidades de planificación

Especifica las modalidades de planificación central que soporta el servidor.

Receptores activos

Especifica los receptores para los que se ha iniciado la anotación de eventos.

¿Gestor de configuración?

Especifica si el servidor es un gestor de configuración.

Intervalo de renovación

Especifica el intervalo que transcurre antes de que el servidor gestionado solicite una renovación de todos los cambios de un gestor de configuración.

Fecha/hora última renovación

Si el servidor es un servidor gestionado, especifica la fecha y la hora de la última renovación ejecutada correctamente de la información de configuración del gestor de configuración.

Envío de mensajes de contexto

Especifica si el envío de mensajes de contexto está activado o desactivado.

Retención de carga de la tabla de contenido (TOC)

Especifica el número aproximado de minutos que se retienen en la base de datos los datos de tabla de contenido sin referencia.

ID exclusivo global de máquina

El identificador exclusivo global (GUID) existente la última vez que se inició el servidor. Este GUID identifica el sistema host al que pertenece el servidor actual.

Protección de retención de copias archivadas

Especifica si la protección de retención de datos de copia archivada está activa.

Directorios de base de datos

Especifica las ubicaciones de los directorios de base de datos.

Espacio total de sistema de archivos (MB)

Especifica el tamaño total del sistema de archivos.

Espacio utilizado en sistema de archivos (MB)

Especifica la cantidad de espacio que se utiliza en el sistema de archivos.

Espacio libre disponible (MB)

Especifica la cantidad de espacio disponible.

Nivel de cifrado

Indica el nivel de cifrado de los datos: AES o DES.

Intervalo de renovación de la información de CPU de cliente

Especifica el número de días transcurridos entre exploraciones de cliente para la información de CPU utilizada para la estimación de PVU.

Réplica de salida

Especifica si el proceso de réplica está activado o desactivado. Si la réplica de salida está desactivada, no pueden iniciarse nuevos procesos de réplica en el servidor.

Servidor de réplica destino

Especifica el nombre del servidor que es el destino de las operaciones de réplica de nodo. Si un servidor de réplica de destino no existe, el campo está en blanco.

Norma de réplica predeterminada para archivado

Especifica la regla de réplica del servidor que se aplica a los datos de archivado. Son posibles los siguientes valores:

ALL_DATA

Replica los datos de archivado. Los datos se replican con una prioridad normal.

ALL_DATA_HIGH_PRIORITY

Replica los datos de archivado. Los datos se replican con una prioridad alta.

NONE

Los datos de archivado no se replican.

Norma de réplica predeterminada para copia de seguridad

Especifica la regla de réplica del servidor que se aplica a los datos de copia de seguridad. Son posibles los siguientes valores:

ALL_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro FORCE_RECONCILE=YES.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL_DATA_HIGH_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE_DATA excepto que los datos se replican con una prioridad alta.

NONE

Los datos de copia de seguridad no se replican.

Norma de réplica predeterminada para gestión de espacios

Especifica la regla de réplica del servidor que se aplica a los datos gestionados por espacio. Son posibles los siguientes valores:

ALL_DATA

Replica los datos gestionados por espacio. Los datos se replican con una prioridad normal.

ALL_DATA_HIGH_PRIORITY

Replica los datos gestionados por espacio. Los datos se replican con una prioridad alta.
NONE

Los datos gestionados por espacio no se replican.

Período de retención de registros de réplicas

Especifica el número de días que se retienen los registros de historial de réplicas en la base de datos del servidor de réplica de origen.

Usuario LDAP

Especifica el ID de usuario que se nombra en el mandato SET LDAPUSER. Este ID de usuario puede emitir mandatos administrativos en el espacio de nombres reservado para IBM Spectrum Protect en el servidor de directorios LDAP.

Establecer contraseña de LDAP

Este campo de salida muestra si se define una contraseña para el ID de usuario que se especifica en el SET LDAPUSER mandato. Los valores son YES y NO. Si es YES, el ID de usuario que se especifica en el mandato SET LDAPUSER puede emitir mandatos administrativos en el espacio de nombres de LDAP que está reservado para IBM Spectrum Protect. Si NO, emita el mandato SET LDAPPASSWORD para definir la contraseña para el ID de usuario que se nombra en el mandato SET LDAPUSER.

Autenticación predeterminada

Especifica el método de autenticación de contraseña predeterminada: LOCAL o LDAP.

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP

Cuando emite el mandato SET DEFAULTAUTHENTICATION define el método de autenticación resultante para todos los mandatos REGISTER ADMIN y REGISTER NODE. El valor predeterminado es LOCAL.

Dirección de alto nivel de migración tras error

Especifica la dirección de alto nivel para el servidor de migración tras error que utiliza el cliente. Las operaciones de restauración de cliente migran tras error en esta dirección de nivel superior cuando la interfaz que utiliza el cliente es distinta a la interfaz utilizada por la réplica.

Retención de anotación

Especifica el número de días para el que se retienen entradas de anotación desde que se actualizó por última vez.

Recuperación de duplicación de archivos dañados

Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino. Este es un valor del lado del sistema. Si se especifica Activado, el proceso de réplica del nodo se puede configurar para detectar los archivos dañados en un servidor de réplica de origen y sustituirlos por archivos sin dañar de un servidor de réplica de destino. Si se especifica Desactivado, los archivos dañados no se recuperan de un servidor de réplica de destino.

Ocupación SUR (TB)

Si tiene una licencia de IBM Spectrum Protect Suite (SUR), este campo especifica la ocupación de SUR en el servidor. La *ocupación SUR* es la cantidad de espacio que se utiliza para almacenar datos que gestionan productos de IBM Spectrum Protect que están incluidos en el paquete SUR.

Fecha y hora de ocupación SUR

Especifica la fecha y hora en las que se recopilaron los datos de ocupación SUR por última vez.

Capacidad inicial (MB)

Especifica la cantidad de datos primarios de los cuales se ha notificado que los clientes están haciendo una copia de seguridad. Los clientes pueden ser aplicaciones, máquinas virtuales y sistemas. Este valor se utiliza para el modelo de licencias frontal.

Recuento del cliente inicial

Especifica el número de clientes que han notificado el uso de la capacidad basado en el modelo de licencias frontales.

Fecha de capacidad inicial

Especifica la fecha y hora cuando se recopilaron por última vez los datos de capacidad inicial.

Oferta de producto

Especifica una oferta de producto.

Valor especificado por el mandato SET PRODUCTOFFERING	Valor mostrado en la salida del mandato QUERY STATUS
ENTry	IBM Spectrum Protect Entry
DATARet	IBM Spectrum Protect para retención de datos
BASIC	IBM Spectrum Protect
EE	IBM Spectrum Protect Extended Edition
SUIte	IBM Spectrum Protect Suite
SUITEEntry	IBM Spectrum Protect Suite Entry
SUITEArchive	IBM Spectrum Protect Suite - Archive
SUITEProtectier	IBM Spectrum Protect Suite - ProtecTier
SUITEFrontend	IBM Spectrum Protect Suite - FrontEnd

Valor especificado por el mandato SET PRODUCTOFFERING	Valor mostrado en la salida del mandato QUERY STATUS
SUITEENTRYFrontend	IBM Spectrum Protect Suite Entry - FrontEnd
CLEAR	NULO

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY STATUS

Mandato	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
SET ACCOUNTING	Especifica si se crean registros de contabilidad al final de cada sesión cliente.
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.
SET CONTEXTMESSAGING	Especifica que debe activarse el envío de mensajes de contexto para depurar un mensaje ANR9999D
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un mandato planificado.
SET MAXSCHEDESESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET PRODUCTOFFERING	Establece la oferta de producto para la que su empresa tiene licencia.
SET QUERYSCHEDPERIOD	Especifica la frecuencia en que los clientes pueden obtener el trabajo planificado, en modalidad por sondeo de cliente.
SET RANDOMIZE	Especifica la aleatorización de las horas de inicio de un margen de las planificaciones en modalidad por sondeo de cliente.

Mandato	Descripción
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
SET SUMMARYRETENTION	Especifica el número de días que se debe mantener la información en la tabla resumen de actividades.
SET TOCLOADRETENTION	Especifica el número de minutos que se debe mantener la información de los conjuntos de tabla de contenido sin referencia.

QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)

Utilice este mandato para visualizar información sobre los umbrales de supervisión de estado.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query STATusthreshold-+-----+-----+-----+----->
                          .-*-----+
                          '-nombre_umbral-'

.-Format----Standard----.
>+-----+-----+-----+-----+-----+-----+----->
  '-Format----+Standard-+-'   '-Activity----+actividad-'
      '-Detailed-'

>+-----+-----+-----+-----+-----+-----+----->
  '-Condition----+EXists-+-'   '-Value----+nombre_valor-'
      +-GT-----+
      +-GE-----+
      +-LT-----+
      +-LE-----+
      '-Equal--'

>+-----+-----+-----+-----+-----+-----+-----><
  '-Status----+Normal-+-'
      +-Warning-+
      '-Error--'

```

Parámetros

nombre_umbral

Especifica el nombre de umbral. El nombre de no puede tener más 48 caracteres de longitud.

Format

Especifica cómo se ha de visualizar la información. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial para los umbrales de estado especificados.

Detailed

Especifica que se visualizará información completa para los umbrales de estado especificados.

actividad

Especifica la actividad para la que desea visualizar indicadores de estado. Si no especifica un valor, se visualizará información para todas las actividades. Para obtener una lista de actividades, consulte el mandato DEFINE STATUSTHRESHOLD.

Condition

Restringe la salida a sólo aquellos que coincidan con el valor especificado. Los valores posibles son:

EXists

Visualiza umbrales de estado donde la condición es igual a EXISTS.

GT

Visualiza umbrales de estado donde la condición es igual a GT.

GE

Visualiza umbrales de estado donde la condición es igual a GE.

LT

Visualiza umbrales de estado donde la condición es igual a LT.

LE

Visualiza umbrales de estado donde la condición es igual a LE.

EQual

Visualiza umbrales de estado donde la condición es igual a EQUAL.

Value

Visualiza umbrales que tienen el valor especificado. Si no especifica un valor, se visualizará información para todos los valores. Puede especificar un entero de 0 a 9223372036854775807.

Status

Visualiza umbrales de estado que tienen el valor de estado especificado. Si no especifica un valor, se visualizará información para todos los valores. Los valores posibles son:

Normal

Visualiza los umbrales de estado que tienen un valor de estado normal.

Aviso

Visualiza los umbrales de estado que tienen un valor de estado de aviso.

Error

Visualiza los umbrales de estado que tienen un valor de estado de error.

QUERY status threshold

Consulte todos los umbrales de estado emitiendo el mandato siguiente:

```
query statusthreshold
```

Nombre umbral	Nomb.actividad	Nombre condición	Valor	Estado informe
-----	-----	-----	-----	-----
ACTIVELOGCHECK	ACTIVE LOG UTILIZATION (%)	>	90	ERROR
AVGSTGPLW	AVERAGE STORAGE POOL UTILIZATION (%)	>	85	WARNING
AVGSTGPLE	AVERAGE STORAGE POOL UTILIZATION (%)	>	90	ERROR

Consultar umbrales de estado y visualizar formato detallado

Consulte los umbrales de estado y visualice la salida en formato detallado, emitiendo el mandato siguiente:

```
query statusthreshold f=d
```

```
Nombre de umbral: ACTIVELOGCHECK
```

```
Nombre de la actividad: ACTIVE LOG UTILIZATION (%)
```


Nombre de la condición: >
 Valor: 90
 Estado del informe: ERROR
 Nombre de servidor: TSMAWP24

Nombre de umbral: AVGSTGPLW
 Nombre de la actividad: AVERAGE STORAGE POOL UTILIZATION (%)
 Nombre de la condición: >
 Valor: 85
 Estado del informe: WARNING
 Nombre de servidor: TSMAWP24

Nombre de umbral: AVGSTGPLE
 Nombre de la actividad: AVERAGE STORAGE POOL UTILIZATION (%)
 Nombre de la condición: >
 Valor: 95
 Estado del informe: ERROR
 Nombre de servidor: TSMAWP24

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY STATUSTHRESHOLD

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

QUERY STGPOOL (Consultar agrupaciones de almacenamiento)

Utilice este mandato para visualizar información acerca de una o varias agrupaciones de almacenamiento. También puede utilizar este mandato para supervisar procesos de migración para agrupaciones de almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query STGpool-+-----+----->
                .-*-----+
                '-nombre_agrupación-'

.-Format----Standard----.
>--+-----+----->
  '-Format----+Standard-+'
                '-Detailed-'
  
```

```

.-POoltype---ANY-----
>-----+-----+-----><
'-POoltype---+ANY-----+'
      +-Primary-----+
      +-COpy-----+
      +-COPYCONtainer-+
      '-ACTIVEdata----'

```

Parámetros

nombre_agrupación

Especifica la agrupación de almacenamiento que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se visualizarán todas las agrupaciones de almacenamiento.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

POoltype

Especifica el tipo de agrupación de almacenamiento que se consulta. Este parámetro es opcional. El valor predeterminado es ANY. Especifique uno de los siguientes valores:

ANY

Se consultan las agrupaciones de almacenamiento primarias, las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos.

PRimary

Sólo se consultan las agrupaciones de almacenamiento primarias.

COpy

Sólo se consultan las agrupaciones de almacenamiento de copia.

COPYCONtainer

Sólo se consultan las agrupaciones de almacenamiento de copia de contenedor.

ACTIVEdata

Sólo se consultan las agrupaciones de almacenamiento de datos activos.

Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de disco de acceso aleatorio

Consejo: En los ejemplos de la salida detallada, algunos campos están en blanco porque el elemento no se aplica en el entorno especificado.

Mostrar detalles para una agrupación de almacenamiento llamada DISKPOOL. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool diskpool format=detailed
```

```

Nombre agrupación almacenamiento: DISKPOOL
Tipo agrupación almacenamiento: Primaria
Nombre de clase de dispositivo: DISK
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 66 G
Desencadenante de espacio: 0,0
  % Util: 0,0
  % Migr: 3,1
  % Lógico: 100,0
  % Migr alto: 90
  % Migr bajo: 70
Retardo migración: 0
Continuar migración: Yes
Procesos migración: 1
Procesos reclamación: 1

```

```

    Siguiente agrupación almacenamiento:
    Agrupación de almacenamiento de reclamación:
    Tamaño máximo umbral: Ilimitado
        Acceso: Lectura/Grabación
        Descripción:
        Ubicación desbordamiento:
        ¿Caché de archivos migrados?:
            ¿Función proximidad?: Grupo
        Umbral reclamación: 60
        Límite de reclamación fuera del local:
        Máximo de volúmenes reutilizables: 32
        Número volúmenes reutilizables utilizados: 1
        Periodo de retardo para reutilización de contenedor: 1 día(s)
        ¿Migración en curso?: No
        Cantidad migrada (MB): 0,00
        Tiempo transcurrido en migración (segundos): 0
        ¿Reclamación en curso?: No

    Última actualización por (administrador): SERVER_CONSOLE
        Fecha/hora última actualización: 01/03/2014 13:57:16
        Formato datos agrupación almacenamiento: nativo
        Agrupaciones almacenamiento copias:
        Agrupaciones de datos activos:
        ¿Continuar la copia en caso de error?: No
        Datos CRC: sí
        Tipo de reclamación: Umbral
        Grabar sobre datos cuando se supriman: 2 veces
        ¿Eliminar duplicados de datos?: No
        Procesos para identificar duplicados:
        Comprimido:
        Ahorro de la deduplicación:
        Ahorro de compresión:
        Espacio total ahorrado:
        Modalidad de copia automática: Cliente
    ¿Contiene eliminaciones de datos duplicados por clientes?: No
        Máximo de grabadores simultáneos:
        Procesos de protección:
        Agrupación de almacenamiento de protección:
        Proteger agrupaciones de almacenamiento locales:
        Límite del volumen de reclamación:

    Fecha de última protección de la agrupación local:
    Fecha de última protección de la agrupación local:
        ¿La eliminación de duplicados requiere una copia seguridad?:
        Cifrada:
        Pct cifrado:
    Espacio de nube asignado (MB):
    Espacio de nube utilizado (MB):
        Nombre de grupo:
    Capacidad estimada local:
        Pct. util local:
        Pct. lógico local:

```

Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de disco de acceso secuencial

Mostrar detalles para una agrupación de almacenamiento denominada FILEPOOL. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool filepool format=detailed
```

```

Nombre agrupación almacenamiento: FILEPOOL
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo: FILEC
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 66 G
Desencadenante de espacio: 0,0
    % Util: 0,0
    % Migr: 3,1
    % Lógico: 100,0
    % Migr alto: 90
    % Migr bajo: 70

```

```

    Retardo migración: 0
    Continuar migración: Yes
    Procesos migración: 1
    Procesos reclamación: 1
    Siguiete agrupación almacenamiento:
    Agrupación de almacenamiento de reclamación:
    Tamaño máximo umbral: Ilimitado
        Acceso: Lectura/Grabación
    Descripción:
    Ubicación desbordamiento:
    ¿Caché de archivos migrados?:
        ¿Función proximidad?: Grupo
    Umbral reclamación: 60
    Límite de reclamación fuera del local:
    Máximo de volúmenes reutilizables: 32
    Número volúmenes reutilizables utilizados: 1
    Periodo de retardo para reutilización de contenedor: 1 día(s)
    ¿Migración en curso?: No
    Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
    ¿Reclamación en curso?: No
    Última actualización por (administrador): SERVER_CONSOLE
    Fecha/hora última actualización: 01/02/2014 13:57:16
    Formato datos agrupación almacenamiento: nativo
    Agrupaciones almacenamiento copias:
    Agrupaciones de datos activos:
    ¿Continuar la copia en caso de error?: No
        Datos CRC: sí
    Tipo de reclamación: Umbral
    Grabar sobre datos cuando se supriman:
    ¿Eliminar duplicados de datos?: Sí
    Procesos para identificar duplicados: 1
        Comprimido:
        Ahorro de deduplicación: 65.396 K (49,99%)
        Ahorro de compresión:
        Espacio total ahorrado: 65.396 K (49,99%)
        Modalidad de copia automática: Cliente
    ¿Contiene eliminaciones de datos duplicados por clientes?: Sí
    Máximo de grabadores simultáneos:
    Procesos de protección:
    Agrupación de almacenamiento de protección:
    Proteger agrupaciones de almacenamiento locales:
    Límite del volumen de reclamación:
    Fecha de última protección de la agrupación local:
    Fecha de última protección de la agrupación local:
    ¿La eliminación de duplicados requiere una copia seguridad?:
        Cifrada:
        Pct cifrado:
    Espacio de nube asignado (MB):
    Espacio de nube utilizado (MB):
        Nombre de grupo:
    Capacidad estimada local:
        Pct. util local:
        Pct. lógico local:

```

Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de acceso secuencial

Mostrar detalles para una agrupación de almacenamiento secuencial de datos activos que se llama FILEPOOL que utiliza una clase de dispositivo de tipo FILE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool filepool format=detailed
```

```

Nombre agrupación almacenamiento: FILEPOOL
Tipo de agrupación de almacenamiento: Datos activo
Nombre clase dispositivo: FILEC
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 0,0 M
Desencadenante de espacio: 0,0
    % Util: 0,0
    % Migr: 0,0

```

```

        % Lógico: 0,0
        % Migr alto: 90
        % Migr bajo: 70
        Retardo migración: 0
        Continuar migración: Yes
        Procesos migración: 1
        Procesos reclamación: 1
        Siguiete agrupación almacenamiento:
        Agrupación de almacenamiento de reclamación:
        Tamaño máximo umbral: Ilimitado
        Acceso: Lectura/Grabación
        Descripción:
        Ubicación desbordamiento:
        ¿Caché de archivos migrados?:
        ¿Función proximidad?: Grupo
        Umbral reclamación: 60
        Límite de reclamación fuera del local:
        Máximo de volúmenes reutilizables: 99
        Número volúmenes reutilizables utilizados: 0
        Período de retardo para reutilización de contenedor: 1 día(s)
        ¿Migración en curso?: No
        Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
        ¿Reclamación en curso?: No
        Última actualización por (administrador): SERVER CONSOLE
        Fecha/hora última actualización: 01/02/2014 11:37:57
        Formato datos agrupación almacenamiento: nativo
        Agrupaciones almacenamiento copias:
        Agrupaciones de datos activos:
        ¿Continuar la copia en caso de error?:
        Datos CRC: sí
        Tipo de reclamación: Umbral
        Grabar sobre datos cuando se supriman:
        ¿Eliminar duplicados de datos?: Sí
        Procesos para identificar duplicados: 1
        Comprimido:
        Ahorro de deduplicación: 65.396 K (49,99%)
        Ahorro de compresión:
        Espacio total ahorrado: 65.396 K (49,99%)
        Modalidad de copia automática:
        ¿Contiene eliminaciones de datos duplicados por clientes?: No
        Máximo de grabadores simultáneos:
        Procesos de protección:
        Agrupación de almacenamiento de protección:
        Proteger agrupaciones de almacenamiento locales:
        Límite del volumen de reclamación:
        Fecha de última protección de la agrupación local:
        Fecha de última protección de la agrupación local:
        ¿La eliminación de duplicados requiere una copia seguridad?:
        Cifrada:
        Pct cifrado:
        Espacio de nube asignado (MB):
        Espacio de nube utilizado (MB):
        Nombre de grupo:
        Capacidad estimada local:
        Pct. util local:
        Pct. lógico local:

```

Ejemplo: visualizar información de resumen acerca de una agrupación de almacenamiento específica

Mostrar información para una agrupación de almacenamiento que se llama POOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool pool1
```

Nombre agrupación	Nombre clase	Capacidad estimada (MB)	% Util	% Migr	% Mig sup.	% Mig inf.	Siguiete agrupación almac. dispositivo
POOL1	DISK	58,5 M	0,8	0,7	90	70	POOL2

Ejemplo: Visualizar información detallada acerca de la agrupación de almacenamiento de cinta de 8 mm

Visualizar los detalles sobre la agrupación de almacenamiento denominada 8MMPool. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool 8mmpool format=detailed
```

```
Nombre agrupación almacenamiento: 8MMPool
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo: 8MMTAPE
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 0,0 M
Desencadenante de espacio: 0,0
  % Util: 0,0
  % Migr:
    % Lógico: 0,0
    % Migr alto: 90
    % Migr bajo: 70
Retardo migración: 0
Continuar migración: Yes
Procesos migración: 1
Procesos reclamación: 1
  Siguiente agrupación almacenamiento:
Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral: 5 M
  Acceso: Lectura/Grabación
  Descripción: Agrupación de
                almacenamiento
                principal
Ubicación desbordamiento: Room1234/Bldg31
¿Caché de archivos migrados?:
  ¿Función proximidad?: No
Umbral reclamación: 60
Límite de reclamación fuera del local:
Máximos volúmenes reutilizables: 5
  Volúmenes reutilizables utilizados: 3
Período de retardo para reutilización de contenedor: 1 día(s)
  ¿Migración en curso?: No
  Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
  ¿Reclamación en curso?: No
Última actualización por (administrador): ADMIN
  Fecha/hora última actualización: 01/08/2014 06:55:45
Formato datos agrupación almacenamiento: nativo
  Agrupaciones de almacenamiento de copia: COPYPOOL1
  Agrupaciones de datos activos: ACTIVEPOOL1 ACTIVEPOOL2
  ¿Continuar la copia en caso de error?: Yes
    Datos CRC: sí
    Tipo de reclamación: Umbral
  Grabar sobre datos cuando se supriman:
    ¿Eliminar duplicados de datos?: No
Procesos para identificar duplicados:
  Comprimido:
  Ahorro de la deduplicación:
  Ahorro de compresión:
  Espacio total ahorrado:
  Comprimido: No
  Ahorro de la deduplicación:
  Ahorro de compresión:
  Espacio total ahorrado:
  Modalidad de copia automática: Cliente
¿Contiene eliminaciones de datos duplicados por clientes?: No
  Máximo de grabadores simultáneos:
  Procesos de protección:
  Agrupación de almacenamiento de protección:
  Proteger agrupaciones de almacenamiento locales:
  Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
```

```
¿La eliminación de duplicados requiere una copia seguridad?:  
  Cifrada:  
    Pct cifrado:  
Espacio de nube asignado (MB):  
  Espacio de nube utilizado (MB):  
    Nombre de grupo:  
  Capacidad estimada local:  
    Pct. util local:  
    Pct. lógico local:
```

Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento NAS2CLASS

Visualizar los detalles sobre la agrupación de almacenamiento NAS2LIBPOOL. Cuando configure esta agrupación de almacenamiento, debe establecer el formato de datos en NETAPPDUMP. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool nas2libpool format=detailed
```

```
Nombre agrupación almacenamiento: NAS2  
Nombre de agrupación de almacenamiento: NAS2LIBPOOL  
Tipo agrupación almacenamiento: Primaria  
Nombre de clase de dispositivo: NAS2CLASS  
  Tipo de almacenamiento: DEVCLASS  
  Tipo de nube:  
    URL de nube:  
  Identidad de nube:  
  Ubicación de nube:  
Capacidad estimada: 0,0 M  
Util. desencadenante de espacio:  
  % Util: 0,0  
  % Migr:  
    % Lógico: 0,0  
  % Migr alto:  
  % Migr bajo:  
Retardo migración:  
Continuar migración:  
Procesos migración:  
Procesos reclamación:  
  Siguiente agrupación almacenamiento:  
  Agrupación de almacenamiento de reclamación:  
Tamaño máximo umbral:  
  Acceso: Lectura/Grabación  
  Descripción:  
  Ubicación desbordamiento:  
¿Caché de archivos migrados?:  
  ¿Función proximidad?: Grupo  
Umbral reclamación:  
Límite de reclamación fuera del local:  
Máximos volúmenes reutilizables: 50  
Número volúmenes reutilizables utilizados: 0  
Período de retardo para reutilización de contenedor: 1 día(s)  
  ¿Migración en curso?:  
    Cantidad migrada (MB):  
  
Tiempo transcurrido en migración (segundos):  
  ¿Reclamación en curso?:  
Última actualización por (administrador): SERVER_CONSOLE  
  Fecha/hora última actualización: 01/02/2014 16:24:43  
Formato datos agrupación almacenamiento: vuelco NetApp  
  Agrupaciones almacenamiento copias:  
  Agrupaciones de datos activos:  
  ¿Continuar la copia en caso de error?: No  
    Datos CRC: No  
  Tipo de reclamación:  
  Grabar sobre datos cuando se supriman:  
  ¿Eliminar duplicados de datos?: No  
Procesos para identificar duplicados:  
  Comprimido:  
  Ahorro de la deduplicación:  
  Ahorro de compresión:  
  Espacio total ahorrado:  
  Modalidad de copia automática: Cliente  
¿Contiene eliminaciones de datos duplicados por clientes?: No  
  Máximo de grabadores simultáneos:
```

```

Procesos de protección:
Agrupación de almacenamiento de protección:
Proteger agrupaciones de almacenamiento locales:
Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
¿La eliminación de duplicados requiere una copia seguridad?:
Cifrada:
Pct cifrado:
Espacio de nube asignado (MB):
Espacio de nube utilizado (MB):
Nombre de grupo:
Capacidad estimada local:
Pct. util local:
Pct. lógico local:

```

Ejemplo: Visualizar información detallada para una agrupación de almacenamiento de contenedores de directorios utilizada para deduplicación de datos

Visualizar detalles para una agrupación de almacenamiento de contenedores de directorios, DPOOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```

query stgpool dpool1 format=detailed

Nombre agrupación almacenamiento: DPOOL1
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo:
Tipo de almacenamiento: Directorio
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 798 G
Util. desencadenante de espacio:
% Util: 3,4
% Migr:
% Lógico: 100,0
% Migr alto:
% Migr bajo:
Retardo migración:
Continuar migración:
Procesos migración:
Procesos reclamación:
Siguiete agrupación almacenamiento:
Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral: Ilimitado
Acceso: Lectura/Grabación
Descripción:
Ubicación desbordamiento:
¿Caché de archivos migrados?:
¿Función proximidad?:
Umbral reclamación:
Límite de reclamación fuera del local:
Máximo permitido de volúmenes reutilizables:
Número de volúmenes reutilizables utilizados:
Período de retardo para reutilización de contenedor: 1 día(s)
¿Migración en curso?:
Cantidad migrada (MB):

Tiempo transcurrido en migración (segundos):
¿Reclamación en curso?:
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 01/02/2014 16:24:43
Formato datos agrupación almacenamiento: nativo
Agrupaciones almacenamiento copias:
Agrupaciones de datos activos:
¿Continuar la copia en caso de error?:
Datos CRC: No
Tipo de reclamación:
Grabar sobre datos cuando se supriman:
¿Eliminar duplicados de datos?: Sí
Procesos para identificar duplicados:
Comprimido: Sí
Espacio utilizado para datos protegidos: 1.599 M

```



```

Total de espacio pendiente: 100 M
Ahorro de deduplicación: 1.331 M (67,56%)
Ahorro de compresión: 194.805 K (29,82%)
Espacio total ahorrado: 1.521 M (77,22%)
Modalidad de copia automática:
¿Contiene datos deduplicados por el cliente?:
Máximo de grabadores simultáneos: Sin límite
Procesos de protección:
Agrupación de almacenamiento de protección: DPOOL2
Proteger agrupaciones de almacenamiento locales:
Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
¿La eliminación de duplicados requiere una copia seguridad?:
Cifrada:
Pct cifrado: 34,56%
Espacio de nube asignado (MB):
Espacio de nube utilizado (MB):
Nombre de grupo:
Capacidad estimada local:
Pct. util local:
Pct. lógico local:

```

Ejemplo: Visualizar información detallada para una agrupación de almacenamiento de contenedores de nubes utilizada para deduplicación de datos

Visualizar detalles para una agrupación de almacenamiento de contenedores de nubes, CPOOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool cpool1 format=detailed
```

```

Nombre agrupación almacenamiento: CPOOL1
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo:
Tipo de almacenamiento: CLOUD
Tipo de nube: SWIFT
URL de nube: http://localhost.local
Identidad de nube: Bailey
Ubicación de nube: ONPREMISE
Capacidad estimada:
Util. desencadenante de espacio:
Pct. util:
% Migr:
% Lógico: 0,0
% Migr alto:
% Migr bajo:
Retardo migración:
Continuar migración:
Procesos migración:
Procesos reclamación:
Siguiente agrupación almacenamiento:
Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral: Ilimitado
Acceso: Lectura/Grabación
Descripción:
Ubicación desbordamiento:
¿Caché de archivos migrados?:
¿Función proximidad?:
Umbral reclamación:
Límite de reclamación fuera del local:
Máximo permitido de volúmenes reutilizables:
Número de volúmenes reutilizables utilizados:
Período de retardo de la reutilización de un volumen: 1
¿Migración en curso?:
Cantidad migrada (MB):

Tiempo transcurrido en migración (segundos):
¿Reclamación en curso?:
Última actualización por (administrador): CODY
Fecha/hora última actualización: 2015-05-28, 10:47:52
Formato datos agrupación almacenamiento: nativo
Agrupaciones almacenamiento copias:
Agrupaciones de datos activos:
¿Continuar la copia en caso de error?:

```

Datos CRC: No
 Tipo de reclamación:
 Grabar sobre datos cuando se supriman:
 ¿Eliminar duplicados de datos?: Sí
 Procesos para identificar duplicados:
 Comprimido: Sí
 Ahorro deduplicación: 9.241 K (89,76%)
 Ahorro compresión: 1.033 K (98,81%)
 Espacio total ahorrado: 10.274 K (99,79%)
 Modalidad de copia automática:
 ¿Contiene datos deduplicados por el cliente?:
 Máximo de grabadores simultáneos: Sin límite
 Procesos de protección:
 Agrupación de almacenamiento de protección:
 Proteger agrupaciones de almacenamiento locales:
 Límite del volumen de reclamación:

 Fecha de última protección de la agrupación local:
 Fecha de última protección de la agrupación local:
 ¿La eliminación de duplicados requiere una copia seguridad?:
 Cifrado: Yes
 Pct cifrado: 34,56%
 Espacio de nube asignado (MB): 4.231
 Espacio de nube utilizado (MB): 4.231
 Nombre de grupo:
 Capacidad estimada local: 168 G
 Pct. util local: 0,1
 Pct. lógico local: 100,0

Descripciones de los campos

Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

Tipo agrupación de almacenamiento

El tipo de agrupación de almacenamiento.

Nombre clase dispositivo

El nombre de la clase de dispositivo asignada a la agrupación de almacenamiento.

Tipo de almacenamiento

El tipo de almacenamiento que está definido para la agrupación de almacenamiento. Se pueden visualizar los siguientes tipos de almacenamiento:

DEVCLASS

La agrupación de almacenamiento especifica una clase de dispositivo que determina el tipo de dispositivo donde se almacenan los datos.

DIRECTORY

La agrupación de almacenamiento crea contenedores lógicos para datos en los directorios del sistema de archivos.

CLOUD

La agrupación de almacenamiento crea contenedores lógicos para datos en un entorno de nube.

Tipo de nube

Para agrupaciones de almacenamiento en la nube, el tipo de plataforma de la nube.

URL de nube

Para agrupaciones de almacenamiento en la nube, el URL para acceder a la nube privada local o a la nube pública externa.

Identidad de nube

Para agrupaciones de almacenamiento en la nube, el ID de usuario para acceder a la nube privada local o a la nube pública externa.

Ubicación de nube

Para agrupaciones de almacenamiento en la nube, indica si la nube es una nube privada local o una nube pública externa.

Capacidad estimada

La capacidad estimada de la agrupación de almacenamiento en megabytes (M) o gigabytes (G).

Para dispositivos DISK, la capacidad estimada es la capacidad de todos los volúmenes de la agrupación de almacenamiento, incluido cualquier volumen que se haya desactivado.

Para agrupaciones de almacenamiento de acceso secuencial, la capacidad estimada es el espacio total estimado de todos los volúmenes de acceso secuencial en la agrupación de almacenamiento, independientemente de su modo de acceso. Se debe utilizar al menos un volumen en una agrupación de almacenamiento de acceso secuencial (ya sea un volumen reutilizable o un volumen privado) para calcular la capacidad estimada.

Para dispositivos de cinta y FILE, la capacidad estimada para la agrupación de almacenamiento incluye los factores siguientes:

- La capacidad de todos los volúmenes reutilizables que ya ha adquirido y puede adquirir la agrupación de almacenamiento. El número de volúmenes reutilizables se define mediante el parámetro MAXSCRATCH en el mandato DEFINE STGPOOL o UPDATE STGPOOL.
- Número total de volúmenes reutilizables disponibles en la biblioteca de cintas.
- La capacidad estimada es el número más pequeño entre el valor MAXSCRATCH y el número total de volúmenes reutilizables disponibles en la biblioteca de cintas.

Los cálculos de la capacidad estimada dependen del espacio disponible de almacenamiento del dispositivo asignado a la agrupación de almacenamiento. Para las agrupaciones de almacenamiento FILE, la capacidad de la agrupación de almacenamiento se reduce si el almacenamiento disponible es menos que el total de espacio estimado de todos los volúmenes FILE de la agrupación de almacenamiento. El valor que se visualiza para la capacidad se reduce por el tamaño de un volumen FILE de manera incremental a medida que el espacio disponible continúa disminuyendo.

Para Centera, este valor representa la capacidad total del dispositivo de almacenamiento Centera que se está consultando.

Util. desencadenante de espacio

Utilización de la agrupación de almacenamiento, calculada por el desencadenante de espacio de la agrupación de almacenamiento, si existe alguno, para esta agrupación de almacenamiento. Puede definir desencadenantes de espacio solo para las agrupaciones de almacenamiento asociadas a tipos de dispositivo DISK o FILE.

Para los dispositivos de acceso secuencial, la utilización del desencadenante de espacio se expresa como un porcentaje del número de bytes utilizados en cada volumen de acceso secuencias relativo al tamaño del volumen, y la capacidad estimada de todos los volúmenes existentes de la agrupación de almacenamiento. No incluye volúmenes reutilizables potenciales. A diferencia del cálculo del porcentaje de utilización, en el cálculo de la utilización del desencadenante de espacio es más preferible la creación de nuevos volúmenes de archivos privados por parte del desencadenante de espacio que la utilización de más volúmenes reutilizables.

Para los dispositivos de disco, la utilización del desencadenante de espacio se expresa en forma de porcentaje de la capacidad estimada, incluidos los datos en caché. Sin embargo, excluye datos que están en cualquier volumen que se haya desactivado. El valor de la utilización del desencadenante de espacio puede ser mayor que el valor del porcentaje de migración si emite el mandato QUERY STGPOOL mientras tiene lugar la creación de un archivo. El valor de la utilización de desencadenante de espacio lo determina la cantidad de espacio asignada mientras la transacción está en curso. El valor del porcentaje de migración representa solo el espacio ocupado por los archivos validados. Al final de la transacción, estos valores se sincronizan.

El valor de la utilización del desencadenante de espacio incluye los datos almacenados en caché en los volúmenes de disco. Por lo tanto, cuando se activa la caché y se produce una migración, el valor permanece igual porque los datos migrados continúan en el volumen como datos en caché. El valor solo disminuye cuando los datos de la memoria caché caducan o cuando el espacio que ocupan los archivos de la memoria caché se deben utilizar para archivos que no están en la memoria caché.

Pct. util

Un cálculo de la utilización de la agrupación de almacenamiento especificado como porcentaje.

Para los dispositivos de acceso secuencial, es un porcentaje del número de bytes activos en cada volumen de acceso secuencial y la capacidad estimada de todos los volúmenes de la agrupación de almacenamiento. El porcentaje incluye el número de volúmenes reutilizables potenciales que se pueden asignar.

Para dispositivos de disco, es un porcentaje de la capacidad estimada, incluyendo los datos en caché y los datos que residen en todos los volúmenes que están desactivados. El valor de Pct Util puede ser mayor que el valor de Pct Migr, si emite este mandato mientras está en proceso una transacción de creación de archivos. El valor de Pct Util se determina por la cantidad de espacio asignado, mientras la transacción está en proceso. El valor de Pct Migr sólo representa el espacio que ocupan los archivos validados. Al final de la transacción, se sincronizan estos valores.

El valor de Pct Util incluye los datos almacenados en caché en los volúmenes de disco. Por lo tanto, cuando se activa la caché y se produce una migración, el valor de Pct Util permanece igual porque los datos migrados continúan en el volumen como datos en caché. El valor de Pct Util sólo disminuye cuando los datos en caché caducan o cuando el espacio que ocupan los archivos en caché debe utilizarse para archivos que no están en caché.

Para Centera, esto representa un cálculo del uso de todo el dispositivo de almacenamiento Centera completo, no el espacio de la agrupación de almacenamiento que se está consultando.

Pct Migr (sólo agrupaciones de almacenamiento primario)

Un cálculo del porcentaje de los datos de la agrupación de almacenamiento que se pueden migrar. El servidor utiliza este valor y el de los umbrales superior e inferior de migración para determinar cuándo debe iniciarse y pararse la migración.

Para dispositivos de disco de acceso aleatorio, este valor se especifica como un porcentaje del valor de la capacidad estimada, excluidos los datos en caché, pero incluidos los datos de todos los volúmenes desactivados.

Para dispositivos de disco de acceso secuencial, este valor se especifica como un porcentaje del valor de la capacidad estimada. Este valor incluye la capacidad de todos los volúmenes reutilizables que se han especificado para la agrupación. Para otros tipos de dispositivos de acceso secuencial, este valor se especifica como el porcentaje del número total de volúmenes de la agrupación de almacenamiento que contienen como mínimo un byte de datos activos. El número total de volúmenes incluye el número máximo de volúmenes reutilizables.

El valor de Pct Util incluye los datos en caché de un volumen; el valor de Pct Migr excluye los datos en caché. Por lo tanto, cuando se activa la caché y se produce una migración, el valor de Pct Migr disminuye pero el valor de Pct Util permanece igual porque los datos migrados permanecen en el volumen como datos en caché. El valor de Pct Util sólo disminuye cuando los datos en caché caducan o cuando el espacio que ocupan los archivos en caché debe utilizarse para archivos que no están en caché.

Pct. lógico

La ocupación lógica de la agrupación de almacenamiento como un porcentaje de la ocupación total. La ocupación lógica es el espacio que ocupan los archivos de cliente que podrían formar parte o no de una agregación de archivos. Un valor de Pct Lógico menor al 100% indica que hay espacio libre en los agregados de archivos de la agrupación de almacenamiento.

Pct. migr alto (sólo agrupaciones de almacenamiento primario)

El umbral superior de migración, que especifica cuándo puede el servidor empezar la migración de la agrupación de almacenamiento. El servidor empieza los procesos de migración cuando la utilización de la capacidad alcanza este umbral.

Pct. migr bajo (sólo agrupaciones de almacenamiento primario)

El umbral inferior de migración, que especifica cuándo puede el servidor terminar la migración de la agrupación de almacenamiento. El servidor detiene los procesos de migración cuando la utilización de la capacidad alcanza este umbral.

Retardo de migración (sólo agrupaciones de almacenamiento primario)

El número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el servidor pueda migrar el archivo a la siguiente agrupación de almacenamiento. Para una agrupación de almacenamiento de disco, los días se cuentan a partir del momento en que el archivo se ha almacenado en la agrupación de almacenamiento o un cliente lo ha recuperado por última vez. Para una agrupación de almacenamiento de acceso secuencial, los días se cuentan a partir del momento en que el archivo se ha almacenado en la agrupación de almacenamiento.

Continuar migración (sólo agrupaciones de almacenamiento primario)

Si el servidor continúa migrando archivos a la siguiente agrupación de almacenamiento aunque los archivos no hayan estado en la agrupación el número de días que especifica el retardo de migración.

Procesos migración

El número de procesos paralelos que se utilizan para migrar archivos desde una agrupación de almacenamiento principal aleatoria o secuencial.

Procesos de reclamación

Número de procesos paralelos utilizados para reclamar los volúmenes de una agrupación de almacenamiento de copia o principal de acceso secuencial.

Siguiente agrupación de almacenamiento (sólo agrupaciones de almacenamiento primario)

La agrupación de almacenamiento que es el destino de los datos que se migran desde esta agrupación de almacenamiento.

Agrupación de almacenamiento de reclamación (sólo agrupaciones de almacenamiento primario de acceso secuencial)

Si se especifica, la agrupación de almacenamiento que es el destino de los datos que se traspasan de los volúmenes durante el proceso de reclamación. Si no se especifica ninguna agrupación, de forma predeterminada, el proceso de reclamación sólo traspasa datos entre los volúmenes de la misma agrupación de almacenamiento.

Umbral de tamaño máximo (sólo agrupaciones de almacenamiento primario)

Tamaño máximo de los archivos que se pueden almacenar en la agrupación de almacenamiento.

Acceso

La modalidad de acceso a los datos de la agrupación de almacenamiento. Son posibles las modalidades de acceso siguientes:

Lectura/ Grabación

Puede accederse a los datos en modalidad de lectura-grabación.

Sólo lectura

Puede accederse a los datos en modalidad de sólo lectura.

Convirtiendo

La agrupación de almacenamiento se está convirtiendo en una agrupación de almacenamiento de contenedores de directorio.

Conversión detenida

El proceso de conversión de la agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio se ha detenido.

Limpieza de conversión necesaria

Para convertir satisfactoriamente la agrupación de almacenamiento, debe limpiarla. La conversión no ha podido completarse porque hay datos dañados. Emita el mandato QUERY CLEANUP para identificar los archivos dañados.

Convertido

La agrupación de almacenamiento se ha convertido en una agrupación de almacenamiento de contenedores de directorio.

Descripción

La descripción de la agrupación de almacenamiento.

Ubicación de desbordamiento)sólo agrupaciones de almacenamiento de acceso secuencial)
La ubicación donde se almacenan los volúmenes de la agrupación de almacenamiento cuando se expulsan de una biblioteca automatizada con el mandato MOVE MEDIA.

¿Archivos migrados en caché? (sólo agrupaciones de almacenamiento de acceso aleatorio)
Si está activada la función de caché para los archivos migrados a la siguiente agrupación de almacenamiento.

¿Función proximidad? (sólo agrupaciones de almacenamiento de acceso secuencial)
Si está desactivada o activada la función de proximidad. Si la función de proximidad está desactivada, el valor de este campo es No. Si la función de proximidad está activada, los valores posibles son Group, Node y Filespace.

Umbral de reclamación (sólo agrupaciones de almacenamiento de acceso secuencial)
El umbral que determina cuándo se reclaman los volúmenes de una agrupación de almacenamiento. El servidor compara con este valor el porcentaje de espacio reclamable que hay en un volumen para determinar si es necesaria la operación de reclamación.

Límite de reclamación fuera del local
El número de volúmenes fuera del local que tienen espacio que se reclama durante la reclamación de esta agrupación de almacenamiento. Este campo se aplica sólo cuando POOLTYPE=COPY.

Máximo de volúmenes reutilizables permitidos (sólo almacenamientos de acceso secuencial)
El número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento.

Número de volúmenes reutilizables utilizados (sólo agrupaciones de almacenamiento de acceso secuencial)
El número de volúmenes reutilizables utilizados en la agrupación de almacenamiento.

Período de retardo para reutilización de contenedor (sólo agrupaciones de almacenamiento de contenedor)
El número de días que deben transcurrir después de suprimir todos los archivos de un contenedor antes de que el servidor reutilice el contenedor.

¿Migración en curso? (sólo agrupaciones de almacenamiento primario)
Si hay como mínimo un proceso de migración activo para la agrupación de almacenamiento.

Cantidad migrada (MB) (sólo agrupaciones de almacenamiento primario)
La cantidad de datos, en megabytes, que se migran, si la migración está en proceso. Si la migración no está en proceso, este valor indica la cantidad de datos migrados durante la última migración. Cuando se utilizan varios procesos de migración paralelos para la agrupación de almacenamiento, este valor indica la cantidad total de datos que migran todos los procesos.

Tiempo transcurrido en migración (segundos) (sólo agrupaciones de almacenamiento primario)
La cantidad de tiempo que ha transcurrido desde que ha empezado la migración, si la migración está activa. Si la migración no está activa, este valor indica la cantidad de tiempo que se necesita para completar la última migración. Cuando se utilizan varios procesos de migración paralelos para la agrupación de almacenamiento, este valor indica la cantidad total de tiempo desde el inicio del primer proceso hasta la finalización del último proceso.

¿Reclamación en curso? (sólo agrupaciones de almacenamiento de acceso secuencial)
Si hay como mínimo un proceso de reclamación activo para la agrupación de almacenamiento.

Última actualización por (administrador)
El nombre del administrador que está definido o que ha actualizado más recientemente la agrupación de almacenamiento.

Fecha/hora última actualización
La fecha y hora en que el administrador ha definido o actualizado más recientemente la agrupación de almacenamiento.

Formato de datos de agrupación de almacenamiento
Tipo de formato de datos utilizado para grabar datos en esta agrupación de almacenamiento (por ejemplo, NATIVE, NETAPPDUMP, CELERRADUMP o NDMPDUMP).

Agrupaciones de almacenamiento de copia
Las agrupaciones de almacenamiento de copia que se enumeran tienen datos que se graban simultáneamente en las mismas cuando se realiza una copia de seguridad de los datos o se archivan dichos datos en una agrupación de almacenamiento primaria consultada mediante este mandato.

Agrupaciones de datos activos
Las agrupaciones de almacenamiento de datos activos que se enumeran aquí tienen datos que se graban simultáneamente en las mismas cuando se realiza una copia de seguridad de los datos en la agrupación de almacenamiento primaria consultada mediante este mandato.

¿Continuar la copia en caso de error?
Indica si un servidor debe continuar grabando datos en otras agrupaciones de almacenamiento de copia de la lista o debe finalizar la transacción por completo cuando se produce un fallo en una de las agrupaciones de copia de la lista. Este campo se aplica únicamente a agrupaciones de almacenamiento de acceso aleatorio y de acceso secuencial primarias.

Datos CRC
Especifica si los datos se validan mediante la comprobación de redundancia cíclica (CRC) cuando se transfieren los datos durante el almacenamiento o la recuperación de datos en un dispositivo.

Tipo de reclamación
Si los volúmenes están reclamado por el umbral o por la fecha de retención de SnapLock.

Grabar sobre datos cuando se supriman
Número de veces que los datos se sobrescriben físicamente después de haberse suprimido de la base de datos.

¿Eliminar duplicados de datos?
Si han de eliminarse o no los datos duplicados de la agrupación de almacenamiento.

Procesos para identificar duplicados

Número de procesos de identificación de duplicados especificado como valor predeterminado para la agrupación de almacenamiento. El número de procesos de identificación de duplicados especificado en este campo podría no ser igual al número de procesos de identificación de duplicados que están en ejecución.

Comprimido

Indica si la agrupación de almacenamiento está comprimida.

Espacio adicional para datos protegidos

La cantidad de espacio, en MB, que se utiliza para proteger datos de los servidores remotos. Se trata de la cantidad total de espacio utilizado para los datos recibidos de otros servidores como resultado de ejecutar el mandato PROTECT STGPOOL.

Después de que se ejecute el mandato PROTECT STGPOOL, los datos no se asignan a un nodo. No obstante, si ejecuta la réplica de nodos en algunos o en todos los nodos, los datos se asignan a los nodos y ya no se asignan al espacio adicional para datos protegidos.

Si no ejecuta la réplica de nodos, los datos recibidos (tras ejecutar el mandato PROTECT STGPOOL) permanecen asignados al espacio adicional para datos protegidos).

Espacio no utilizado total pendiente

La cantidad de espacio que está planificado para que vuelva a estar disponible en una agrupación de almacenamiento de contenedor de directorio. El espacio lo ocupan las extensiones con datos eliminados que se suprimirán de la agrupación de almacenamiento cuando caduque el periodo de tiempo especificado mediante el parámetro REUSEDELAY en el mandato DEFINE STGPOOL.

Ahorro de deduplicación

La cantidad y el porcentaje de datos que se conseguido ahorrar en la agrupación de almacenamiento mediante la deduplicación de datos.

Ahorro de compresión

La cantidad de datos que se ha ahorrado en la agrupación de almacenamiento mediante la compresión.

Espacio total ahorrado

La cantidad total de datos que se ha ahorrado en la agrupación de almacenamiento.

Modalidad de copia automática

Indica si los datos se graban de forma simultánea en agrupaciones de almacenamiento de copia o de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor, los procesos de migración de datos del servidor o las tres operaciones. El valor CLIENT indica operaciones de almacenamiento del cliente o de importación del servidor. El valor ALL indica que la grabación simultánea se produce cuando esta agrupación es el destino de cualquiera de las operaciones elegibles.

Si la agrupación de almacenamiento es una agrupación de almacenamiento de copia o una agrupación de datos activos o si la función de grabación simultánea está inhabilitada, este campo está vacío.

¿Contiene eliminaciones de datos duplicados por clientes?

Indica si la agrupación de almacenamiento contiene datos cuyos duplicados han eliminado los clientes. Los agentes de almacenamiento V6.1 o anteriores no pueden acceder a las agrupaciones de almacenamiento que contienen eliminaciones de datos realizadas por los clientes para el traspaso de datos fuera de la LAN.

Consejo: Este campo está en blanco para agrupaciones de almacenamiento de contenedor. No puede utilizar las agrupaciones de almacenamiento de contenedores para el movimiento de datos sin LAN.

Máximo de grabadores simultáneos

El número máximo de E/S que pueden ejecutarse simultáneamente en la agrupación de almacenamiento.

Procesos de protección

El conjunto de procesos de protección.

Agrupación de almacenamiento de protección

El nombre de la agrupación de almacenamiento de contenedores donde se protegen los datos en el servidor de réplica de destino.

Protección de agrupaciones de almacenamiento local

Indica si las agrupaciones de almacenamiento local están protegidas.

Límite del volumen de reclamación

En el caso de agrupaciones de almacenamiento de copia de contenedor, indica el número máximo de volúmenes que reclama el servidor durante la protección de la agrupación de almacenamiento.

Fecha de última protección de la agrupación remota

La fecha en que se protegió por última vez la agrupación de almacenamiento en una agrupación de almacenamiento de un servidor remoto.

Fecha de última protección en agrupación local

La fecha en que se protegió por última vez la agrupación de almacenamiento en una agrupación de almacenamiento de un servidor local.

¿Necesita una copia de seguridad para eliminar los archivos duplicados?

Indica si debe realizarse una copia de seguridad de la agrupación de almacenamiento secuencial si la agrupación de almacenamiento contiene datos con duplicados eliminados.

Cifrado

Para las agrupaciones de contenedores de directorio o de almacenamiento en la nube, indica si los datos de cliente se cifran antes de que se graben en la agrupación de almacenamiento.

Pct cifrado

El porcentaje de datos de cliente desduplicados que se han cifrado en la agrupación de almacenamiento en la nube de contenedores de directorio o de contenedor en la nube.

Espacio de nube asignado (MB)

Para las agrupaciones de almacenamiento en la nube, la cantidad de espacio que se asigna al almacenamiento en la nube, en megabytes.

Espacio de nube utilizado (MB)

Para las agrupaciones de almacenamiento de nube, esto es el espacio utilizado por la agrupación, expresado en megabytes.

Nombre de grupo

En el caso de agrupaciones de almacenamiento en la nube que utilizan Simple Storage Service (S3), el nombre que IBM Spectrum Protect asigna al grupo de S3 o la caja fuerte de IBM® Cloud Object Storage. Este valor también puede ser el nombre que ha asignado al grupo utilizando el parámetro BUCKETNAME en el mandato DEFINE STGPOOL o en el mandato UPDATE STGPOOL.

Capacidad estimada local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, la capacidad estimada de almacenamiento local en megabytes (M) o gigabytes (G).

Pct. util local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, una estimación del uso del componente de almacenamiento local de la agrupación de almacenamiento en la nube, como un porcentaje.




Pct. lógico local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, la ocupación lógica de la agrupación de almacenamiento en la nube como un porcentaje del total de la ocupación. La ocupación lógica es el espacio que ocupan los archivos de cliente que podrían formar parte o no de una agregación de archivos. Un valor de Pct Lógico local menor que un 100% indica que hay espacio libre en los agregados de la agrupación de almacenamiento.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY STGPOOL

Mandato	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
COPY ACTIVE DATA	Copia los datos de copia de seguridad activos.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

QUERY STGPOOLDIRECTORY (Consulta de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para visualizar información acerca de uno o varios directorios de agrupaciones de almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-*-----.  
>>-Query STGPOOLDirectory--+----->  
      '-directorio-'  
  
>--+----->  
      '-STGpool----nombre_agrupación-'  
  
.Access----Any-----.  
>--+----->  
      '-Access-----READWrite---+'  
          +-READOnly----+  
          +-DEStroyed---+  
          +-Any-----+  
          '-UNAVailable-'  
  
.Format----Standard----.  
>--+-----><  
      '-Format-----Standard+-+'  
          '-Detailed-'
```

Parámetros

directorio

Especifica el directorio de agrupaciones de almacenamiento que se consulta. Este parámetro es opcional.

*

Especifica que un asterisco (*) representa un carácter comodín. Utilice los caracteres comodín como, por ejemplo, un asterisco para que coincida con cualquier carácter. De forma alternativa, puede utilizar un signo de interrogación (?) o un signo de porcentaje (%) para hacer coincidir con exactitud un carácter. Este es el valor predeterminado.

directorio

Especifica el directorio de la agrupación de almacenamiento. Si no especifica un valor para este parámetro, se visualizarán todos los directorios de agrupaciones de almacenamiento. La longitud máxima del directorio de la agrupación de almacenamiento es de 1024.

STGpool

Especifica el nombre de la agrupación de almacenamiento que se va a consultar. Si no especifica un valor para este parámetro, se visualizarán todos los directorios de agrupaciones de almacenamiento. La longitud máxima del nombre de la agrupación de almacenamiento es de 30. Este parámetro es opcional.

ACCess

Especifica que la salida está restringida por la modalidad de acceso de directorio. Este parámetro es opcional. Especifique uno de los siguientes valores:

READWrite

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `READWRITE`.

READOnly

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `READONLY`.

DEStroyed

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `DESTROYED`. Los directorios se han designado como dañados permanentemente en el directorio de la agrupación de almacenamiento.

Any

Visualizar todos los directorios de agrupación de almacenamiento. Este es el valor predeterminado.

UNAVailable

Visualizar directorios con una modalidad de acceso `UNAVAILABLE`.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es `STANDARD`. Puede especificar uno de los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

Ejemplo: Visualización de información de resumen acerca de un directorio específico de agrupaciones de almacenamiento

Visualice información del directorio de agrupaciones de almacenamiento denominado DPOOL. Consulte Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpooldirectory C:\data
```

Storage Pool Name	Directory	Access
DPOOL	C:\data	Read/Write


Ejemplo: Visualización de información detallada del directorio de agrupaciones de almacenamiento

Visualizar detalles del directorio de agrupaciones de almacenamiento denominado DPOOL.

```
query stgpooldirectory stgpool=dpool format=detailed
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
Nombre agrupación almacenamiento: DPOOL
Directorio: /storage/sampleDir
Acceso: Lectura/Grabación
Espacio libre (MB): 323,170
Total espacio (MB): 476,938
Sistema de archivos: /storage
Vía de acceso absoluta: /storage/data
```

 Sistemas operativos Windows

```
Nombre agrupación almacenamiento: DPOOL
Directorio: /storage2/sampleDir
Acceso: Lectura/Grabación
Espacio libre (MB): 323,170
Total espacio (MB): 476,938
Sistema de archivos: /storage
Vía de acceso absoluta: /storage2/sampleDir
```

Descripciones de los campos

Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

Directorio

El nombre del directorio de la agrupación de almacenamiento.

Acceso

La modalidad de acceso de los datos en el directorio de la agrupación de almacenamiento.

Espacio libre (MB)

La cantidad de espacio en el directorio de agrupaciones de almacenamiento, en megabytes, que no se utiliza.

Espacio total (MB)

La cantidad total de espacio en el directorio de agrupaciones de almacenamiento, en megabytes.










Sistema de archivos

El nombre del sistema de archivos donde se halla el directorio de agrupaciones de almacenamiento.

Vía de acceso absoluta

El nombre de la vía de acceso absoluta donde se halla el directorio de agrupaciones de almacenamiento. El nombre de la vía de acceso absoluta contiene el nombre del directorio raíz y todos los subdirectorios en el nombre de la vía de acceso. Todos los enlaces simbólicos se resuelven en el nombre de vía de acceso absoluta.

Tabla 1. Mandatos relacionados con QUERY STGPOOLDIRECTORY

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

QUERY STGRULE (Visualizar información de reglas de almacenamiento)

Utilice este mandato para mostrar información sobre el tipo de regla de almacenamiento definida para una agrupación de almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query STGRULE--.*-----
                    +-----+----->
                    '-nombre_regla-'

.-Format-----Standard-----.-ACTiotype-----ANY-----.
>+-----+-----+-----+----->
  '-Format-----+Standard-+-' '-ACTiotype-----+ANY-+-'
                    '-Detailed-'                '-TIER-'

.-ACTIVE-----ANY-----.
>+-----+-----+-----+-----<
  '-ACTIVE-----+ANY-+-'
                    +-Yes-+
                    '-No--'
    
```

Parámetros

nombre_regla

Especifica el nombre de la regla de almacenamiento. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se visualizarán todas las reglas de almacenamiento. La longitud máxima del nombre es de 30 caracteres.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

ACTiotype

Especifica la acción de almacenamiento que se completa con las reglas de almacenamiento. Son posibles los siguientes valores:

ANY

Se visualizan todos los tipos de reglas de almacenamiento.

TIER

Se visualizan las reglas de almacenamiento por niveles.

ACTIVE

Especifica que se muestran las reglas de almacenamiento activas. Este parámetro es opcional. El valor predeterminado es ANY. Son posibles los siguientes valores:

ANY

Especifica que se muestran todas las reglas de almacenamiento.

YES

Especifica que sólo se muestran las reglas de almacenamiento activas.

NO

Especifica que sólo se muestran las reglas de almacenamiento inactivas.

Ejemplo: Listar todas las reglas de almacenamiento de todas las agrupaciones de almacenamiento

Consultar todas las reglas de almacenamiento para todas las agrupaciones de almacenamiento. Consulte el apartado QUERY STGRULE (Visualizar información de reglas de almacenamiento) para obtener las descripciones de los campos.

```
query stgrule
```

Regla almacenam. archivos	Agrup. destino almac. del cliente	Tipo de regla	Activa	Agrup. almacenamiento origen
STGACTION1	Nube	Nivel	Sí	DIRPOOL1

Ejemplo: visualizar información detallada acerca de una regla de almacenamiento

Consultar información detallada de una regla de almacenamiento para una agrupación de almacenamiento. Crear la salida en formato detallado. Consulte el apartado QUERY STGRULE (Visualizar información de reglas de almacenamiento) para obtener las descripciones de los campos.

```
query stgrule format=detailed
```

```
Nombre de regla: STGACTION1
Agrup. almac. destino: CLOUD
Tipo acción: Nivel
Activa: Sí
Nº máx. de procesos: 8
Hora inicio: 15:00:00
Retardo de nivel (días): 30
Duración:
Descripción: Regla de almacenamiento para nivel de datos
Agrup. de almac. origen: DIRPOOL1
```

Descripciones de los campos

Nombre de regla de almacenamiento

El nombre de la regla de almacenamiento.

Agrupación de almacenamiento de destino

El nombre de la agrupación de almacenamiento de contenedor en la nube.

Tipo de acción

El tipo de regla de almacenamiento.

Activo

Indicación de si la regla de almacenamiento está activa o inactiva.

Número máximo de procesos

El número máximo de procesos por agrupación de almacenamiento de origen.

Hora de inicio

La hora de inicio diaria de la ventana de tiempo en que se ejecuta la regla de almacenamiento.

Retardo de nivel (en días)

El número mínimo de días que el objeto debe permanecer en una agrupación de almacenamiento de origen antes de que la regla de almacenamiento mueva el objeto a la agrupación de almacenamiento de destino.

Duración

El número de minutos durante los que la regla de almacenamiento procesa los datos cuando se han completado todos los procesos asociados. La ausencia de valor indica que el proceso continúa hasta completarse.

Descripción

Una descripción de la regla de almacenamiento.

Agrupaciones de almacenamiento de origen

El nombre de la agrupación o agrupaciones de almacenamiento desde los que la regla mueve los objetos.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY STGRULE

Mandato	Descripción
DEFINE STGRULE	Define una regla de almacenamiento para las agrupaciones de almacenamiento.
DELETE STGRULE	Suprimir reglas de almacenamiento para las agrupaciones de almacenamiento.
UPDATE STGRULE	Actualiza una regla de almacenamiento para las agrupaciones de almacenamiento.

QUERY SUBSCRIBER (Visualizar información de suscriptor)

Utilice este mandato en un gestor de configuración para visualizar información sobre los suscriptores y sus inscripciones en perfiles.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
      .-*-----.  
>>-Query SUBSCRIBer--+-----+----->  
      '-nombre_servidor-'  
  
      .-PROFIle----*-----.  
>--+-----+-----<<  
      '-PROFIle----nombre_perfil-'
```

Parámetros

nombre_servidor

Especifica el nombre de un servidor gestionado para el que se visualiza la información de inscripción. Puede utilizar caracteres comodín para especificar varios nombres de servidores. Este parámetro es opcional. El valor predeterminado son todos los servidores gestionados.

PROFIle

Especifica un nombre de perfil para el que se visualiza la información. Puede utilizar caracteres comodín para especificar varios nombres de perfiles. Este parámetro es opcional. El valor predeterminado son todos los perfiles.

Ejemplo: obtener una lista de las suscripciones de perfil de un gestor de configuración

Visualizar la información de los suscriptores de todas las inscripciones en perfiles para este gestor de configuración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query subscriber
```

Suscriptor	Nombre perfil	¿Actual?	Última actualización actualización
-----	-----	-----	-----
SERVER2	DEFAULT_PROFILE	Si	Jue, 14 Mayo 1998 01:14:42 PM
SERVER2	SETUP	Si	Jue, 14 Mayo 1998 01:14:42 PM

Descripciones de los campos

Suscriptor

El nombre del suscriptor (servidor gestionado).

Nombre de perfil

El nombre del perfil.

¿Es actual?

Si la inscripción se ha renovado con la información actual asociada al perfil. Los valores posibles son:

- Sí
El servidor gestionado es actual.
 - No
El servidor gestionado no es actual. Si este campo tiene el valor NO una vez renovado el perfil, compruebe si en los mensajes del servidor hay condiciones de error que puedan ocasionar que no se haya ejecutado la renovación.
 - Desconocido
El servidor gestionado tiene una versión más reciente del perfil que el gestor de configuración, o bien, el perfil ya no existe en el gestor de configuración, pero la inscripción sigue estando asociada al perfil.
- Fecha/hora última actualización
Especifica la fecha y la hora en que se ha distribuido correctamente al suscriptor la información de configuración para la inscripción.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SUBSCRIBER

Mandato	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

QUERY SUBSCRIPTION (Visualizar información de inscripción)

Utilice este mandato en un servidor gestionado para visualizar la información de suscripción de un perfil.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query SUBSCRIPTION--+-----+-----><
                        .*-----
                        '-nombre_perfil-'

```

Parámetros

nombre_perfil
Especifica el nombre del perfil sobre el que se visualiza información de inscripciones. Puede utilizar caracteres comodín para especificar varios nombres. Este parámetro es opcional. El valor predeterminado son todos los perfiles.

Ejemplo: visualizar información de descripción

Visualizar la información de inscripción de todos los perfiles.

```

query subscription

Gestor          Nombre perfil          Fecha/hora
configuración   -----                últ. act.
-----
SERVER1         ADMIN_INFO              Jue, 14 Mayo 1998
                                01:35:13 PM
SERVER1         DEFAULT_PROFILE        Jue, 14 Mayo 1998
                                01:35:13 PM
SERVER1         EMPLOYEE                Jue, 14 Mayo 1998
                                01:35:13 PM

```

Descripciones de los campos

Gestor de configuración

El nombre del gestor de configuración.

Nombre de perfil

El nombre del perfil.

Fecha/hora última actualización

El momento en que se ha distribuido correctamente la información de configuración más reciente al suscriptor.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SUBSCRIPTION

Mandato	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.

QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)

Utilice este mandato para obtener información consolidada acerca de la configuración y la capacidad del servidor.

Este mandato consolida la salida de sentencias select, mandatos SHOW, y otros mandatos de IBM Spectrum Protect. La salida se genera desde varios mandatos de IBM Spectrum Protect, por ejemplo:

- QUERY ASSOCIATION
- QUERY COPYGROUP
- QUERY DATAMOVER
- QUERY DB
- QUERY DBSPACE
- QUERY DEVCLASS
- QUERY DIRSPACE
- QUERY DOMAIN
- QUERY LIBRARY
- QUERY LOG
- QUERY MGMTCLASS
- QUERY OPTION
- QUERY PROCESS
- QUERY REPLRULE
- QUERY SCHEDULE
- QUERY SERVER
- QUERY SESSION
- QUERY STATUS
- QUERY STGPOOL
- QUERY VOLHISTORY
- QUERY VOLUME

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query SYStem-----<<
```

Ejemplo: visualizar información consolidada del sistema

Emita el mandato QUERY SYSTEM para obtener información consolidada acerca del sistema. Para obtener ejemplos de salidas de estos mandatos de consulta, consulte los mandatos individuales.

```
query system
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY SYSTEM

Mandato	Descripción
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY LOG	Visualiza información acerca de las anotaciones de recuperación.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.

QUERY TAPEALERTMSG (Visualizar estado del mandato SET TAPEALERTMSG)

Utilice este mandato para visualizar el estado del mandato SET TAPEALERTMSG. Puede activar o desactivar las alertas de cinta. Si se activan, IBM Spectrum Protect puede recuperar información de diagnóstico de un dispositivo de cinta o biblioteca y visualizarla mediante mensajes ANR. Si se desactivan, IBM Spectrum Protect no consultará ningún dispositivo para obtener esta información.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-Query TAPEAlertmsg-----<<
```

Ejemplo: visualizar el estado del mandato QUERY TAPEALERTMSG

Utilizar el mandato QUERY TAPEALERTMSG para determinar si deben recuperarse las alertas de cinta de los dispositivos y visualizarse en forma de mensajes ANR.

```
query tapealertmsg
```

```
ANR2017I El administrador SERVER_CONSOLE
         emitió el mandato:
         QUERY TAPEALERTMSG
ANR8960I QUERY TAPEALERTMSG: la visualización de alertas de cinta de
         dispositivos SCSI
         está Activada.
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY TAPEALERTMSG

Mandato	Descripción
SET TAPEALERTMSG	Especifica si los dispositivos de cinta y biblioteca reportan la información de diagnóstico al servidor.

QUERY TOC (Visualizar tabla de contenido para una imagen de copia de seguridad)

Utilice este mandato para visualizar la información sobre los directorios y archivos que contiene la tabla de contenido (TOC) para una imagen de copia de seguridad especificada. Este mandato no carga la información de la tabla de contenido en la base de datos de IBM Spectrum Protect. La tabla de contenido especificada se lee desde una agrupación de almacenamiento cada vez que se emita el mandato QUERY TOC.

Este mandato no se puede emitir desde la consola del servidor. Si la tabla de contenido está almacenada en un medio extraíble, se necesita un punto de montaje y la salida se retardará mientras se monte el volumen de agrupación de almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política para el dominio al que está asignado el nodo o autorización de propietario de cliente en el nodo.

Sintaxis

```
>>-Query TOC--nombre_nodo--nombre_espacioarchivos----->
>--+-----+----->
  '-CREATIONDate----fecha--CREATIONTime----hora-'
  .-Format----Standard----.
>--+-----+-----<
  '-Format----+Standard+-'
    '-Detailed-'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo NAS al que pertenece la tabla de contenido (TOC). No puede utilizar caracteres comodín para especificar este nombre.

nombre_espacio_archivos (Obligatorio)

Especifica el nombre del espacio de archivos al que pertenece la tabla de contenido. El nombre de espacio de archivos especificado no puede contener caracteres comodín.

CREATIONDate

Especifica la fecha de creación de la imagen de copia de seguridad para la que debe visualizarse la tabla de contenido. Este parámetro es opcional. Si especifica CREATIONDATE, también debe especificar CREATIONTIME. Si no especifica estos parámetros, se mostrará el contenido de la imagen de copia de seguridad más reciente para el nodo y el espacio de archivos especificados, siempre que esta imagen tenga una tabla de contenido. Sólo puede especificar la fecha de creación como uno de los valores siguientes:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	05/15/2002

Especifica que desea visualizar el contenido de la imagen de copia de seguridad creada en esta fecha. Puede obtener esta fecha de la salida del mandato QUERY NASBACKUP.

CREATIONTime

Especifica la hora de creación de la imagen de copia de seguridad para la que debe visualizarse la tabla de contenido. Este parámetro es opcional. Si especifica CREATIONTIME, también debe especificar CREATIONDATE. Si no especifica estos parámetros, se mostrará el contenido de la imagen de copia de seguridad más reciente para el nodo y el espacio de archivos especificados, siempre que esta imagen tenga una tabla de contenido. Sólo puede especificar la hora de creación como uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha de creación especificada	10:30:08

Especifica que desea visualizar el contenido de la imagen de copia de seguridad creada a esta hora para la fecha especificada. Puede obtener esta hora en la salida del mandato QUERY NASBACKUP.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial para los archivos.

Detailed

Especifica que se visualizará información completa para los archivos, incluida la representación hexadecimal de cada nombre de archivo o directorio.

Ejemplo: visualizar información de tabla de contenido detallada para un nodo específico

Utilice el mandato QUERY TOC para visualizar la información de la tabla de contenido que pertenece al nodo NAS NETAPP del espacio de archivos /vol/vol1 creado el 12/06/2002 a las 11:22:46. Especificar un formato detallado.

```
query toc netapp /vol/vol1 creationdate=12/06/2002 creationtime=11:22:46
format=detailed
```

Objetos en la imagen de la que se ha realizado una copia el 12/06/2002 a las 11:22:46 para el espacio de archivos /vol/vol1 en el nodo NETAPP:

```

Nombre de objeto: /.etc
Nombre de objeto hexadecimal: 2f657463
Tipo objeto: Directorio
Tamaño objeto: 4.096
Fecha/hora de última modificación de datos: 07/31/2002 14:21:19

Nombre de objeto: /.etc/oldmaps/ndmp
Nombre de objeto hexadecimal: 2f6574632f6f6c646d6170
732f6e646d70
Tipo objeto: Directorio
Tamaño objeto: 4.096
Fecha/hora de última modificación de datos: 07/31/2002 14:21:19

Nombre de objeto: /.etc/oldmaps/ndmp/
TSM
/vol/vol1/3df0e8fd
Nombre de objeto hexadecimal: 2f6574632f6f6c646d6170
732f6e646d702f54534d2
02f766f6c2f766f6c312f3
364663065386664
Tipo de objeto: Archivo
Tamaño de objeto: 36,864
Fecha/hora de última modificación de datos: 12/06/2002 11:14:22
```

Descripciones de los campos

Nombre de objeto

Nombre del objeto.

Nombre de objeto hexadecimal

Nombre del objeto en formato hexadecimal.
 Tipo de objeto
 Tipo de objeto.
 Tamaño de objeto
 Tamaño del objeto.
 Fecha/hora de última modificación de datos
 Fecha y hora de la última modificación del objeto.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY TOC

Mandato	Descripción
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
RESTORE NODE	Restaura un nodo de almacenamiento conectado a red (NAS).

QUERY VIRTUALFSMAPPING (Consultar una correlación de espacios de archivos virtuales)

Utilice este mandato para consultar una definición de correlación de espacios de archivos virtuales.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-Query VIRTUALFSmapping ----->
. -*-----
>-----<
|          .-*-----|
|'-nombre_nodo-----|
|          '-nombre_espacio_archivos_virtual-'
```

Parámetros

nombre_nodo

Especifica el nodo de cliente al que pertenece el espacio de archivos virtual. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado es especificar todos los nombres de nodo. Debe especificar un valor para este parámetro si especifica un nombre de espacio de archivos virtual.

nombre_espacio_archivos_virtual

Especifica el nombre de las correlaciones de espacios de archivos virtuales que consultará. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. Si no especifica ningún valor, se consultan todas las correlaciones de espacios de archivos virtuales. Los nombres de correlaciones de espacios de archivos virtuales son sensibles a las mayúsculas/minúsculas. Utilice el mandato QUERY VIRTUALFSMAPPING para determinar el uso correcto de mayúsculas/minúsculas para la correlación de espacios de archivos virtuales que va a consultarse.

Ejemplo: visualizar los espacios de archivos virtuales para un nodo específico

Visualizar los espacios de archivos virtuales definidos actualmente para el nodo NAS1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query virtualfsmapping nas1
```

```
Nombre  Nombre correlación Nombre      Ruta      ¿Ruta
nodo    de espacios de      espacio   Ruta      hexadecimal?
        archivos virtuales archivos
-----
```

NAS1	/mikesdir	/vol/vol2	/mikes	No
NAS1	/tmpdir	/vol/vol1	/tmp	No
NAS1	/nonASCIIIDir	/vol/vol3	2f73657276657231	Si

Descripciones de los campos

Node Name

Especifica el nombre del nodo cliente.

Virtual Filespace Mapping Name

Especifica el nombre de la correlación de espacios de archivos virtuales.

Filespace Name

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Ruta

Especifica la ruta al nodo de cliente.

Hexadecimal Path

Indica si la ruta es hexadecimal.

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY VIRTUALFSMAPPING

Mandato	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

QUERY VOLHISTORY (Visualizar información histórica de volúmenes secuenciales)

Utilice este mandato para visualizar la información histórica de volúmenes secuenciales. Para guardar la información histórica de volúmenes secuenciales en uno o varios archivos, utilice el mandato BACKUP VOLHISTORY.

Utilice la opción de servidor VOLUMEHISTORY para especificar uno o varios archivos históricos de volúmenes. Una vez reiniciado el servidor, IBM Spectrum Protect actualiza la información de volúmenes en la base de datos y en los archivos.

Utilice el mandato QUERY BACKUPSET para consultar la información correspondiente al conjunto de copias de seguridad especificado.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-BEGINDate-----fecha_anterior-.
>>-Query VOLHistory----->
'-BEGINDate-----fecha-----'
.-ENDDate-----fecha_actual-. .-BEGINTime-----00:00:00-.
```

```

>-----+-----+----->
'-ENDDate---fecha-----' '-BEGINTime---hora-----'

.-ENDTime---hora_actual-. .-Type---All-----
>-----+-----+-----<
'-ENDTime---hora-----' '-Type---+All-----'
      +-BACKUPSET---+
      +-DBBackup----+
      +-DBRpf-----+
      +-DBSnapshot--+
      +-EXPort-----+
      |           (1) |
      +-REmote-----+
      +-RPFile-----+
      +-RPFSnapshot++
      +-STGDelete---+
      +-STGNew-----+
      '-STGReuse----'

```

Notas:

1. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.

Parámetros

BEGINDate

Especifica que desea visualizar la información empezando por los registros creados en la fecha especificada. Este parámetro es opcional. El valor predeterminado es la fecha más antigua en la que existe información histórica.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados	TODAY-7 o -7. Para visualizar la información empezando por los registros creados hace una semana, especifique BEGINDATE=TODAY-7 o BEGINDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDDate

Especifica que desea visualizar la información acabando por los registros creados en la fecha especificada. Este parámetro es opcional. El valor predeterminado es la fecha actual.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-1 o -1. Para visualizar los registros creados hasta ayer, especifique ENDDATE=TODAY-1 o ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica que desea visualizar la información empezando por los registros creados a la hora especificada. Este parámetro es opcional. El valor predeterminado es medianoche (00:00:00).

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	12:33:28
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+03:00 o BEGINTIME=+03:00, IBM Spectrum Protect visualizará los registros que tengan la hora 12:00:00 o posterior, en la fecha inicial especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con BEGINTIME=NOW-03:30 o BEGINTIME=-03:30, IBM Spectrum Protect visualizará los registros que tengan la hora 5:30 o posterior en la fecha inicial.

ENDTime

Especifica que desea visualizar la información acabando por los registros creados a la hora especificada en la fecha final. Este parámetro es opcional. El valor predeterminado es la hora actual.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con ENDTIME=NOW+03:00 o ENDTIME=+03:00, IBM Spectrum Protect visualizará los registros que tengan la hora 12:00 o posterior, en la fecha final.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30 Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME=-3:30, IBM Spectrum Protect visualizará los registros que tengan la hora 5:30 o anterior, en la fecha final.

Type

Especifica el tipo de registros a visualizar del archivo histórico de volúmenes. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

All	Especifica todos los registros.
BACKUPSET	Especifica que se visualizará sólo la información sobre los volúmenes de juego de copias de seguridad.
DBBackup	Especifica que sólo se visualizarán los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos, es decir, los tipos de volumen BACKUPFULL y BACKUPINCR.
DBRpf	Especifica que sólo se visualizarán los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos y los volúmenes de objetos del archivo del plan de recuperación (los tipos de volúmenes BACKUPFULL, BACKUPINCR y RPFfile).
DBSnapshot	Especifica que se visualizarán sólo los registros que contienen información sobre los volúmenes utilizados para las copias de seguridad de instantánea de base de datos.
EXPort	Especifica sólo los registros que contienen información sobre los volúmenes de exportación.
REMote	Especifica que sólo se visualizarán los registros que contienen información acerca de los volúmenes que los clientes de biblioteca han utilizado.
RPFfile	Especifica que sólo se muestren los registros que contienen información sobre los objetos de archivos de un plan de recuperación que están guardados en un servidor de destino y que se han creado presuponiendo copias de seguridad de base de datos completas e incrementales. El parámetro muestra sólo los registros de los archivos de plan de recuperación que se han guardado en otro servidor IBM Spectrum Protect utilizando la función de volumen virtual de servidor a servidor para IBM Spectrum Protect.
RPFSnapshot	Especifica que sólo se muestren los registros que contienen información sobre los objetos de archivos de un plan de recuperación que están guardados en un servidor de destino y que se han creado suponiendo copias de seguridad de instantánea de base de datos. RPFSnapshot sólo visualiza registros acerca de archivos de plan de recuperación que se han guardado en otro servidor IBM Spectrum Protect utilizando la función de volumen virtual de servidor a servidor para IBM Spectrum Protect.
STGDelete	Especifica sólo los registros que contienen información sobre los volúmenes de agrupaciones de almacenamiento secuenciales suprimidos.
STGNew	Especifica sólo los registros que contienen información sobre los nuevos volúmenes de almacenamiento de acceso secuencial.
STGReuse	Especifica sólo los registros que contienen información sobre los volúmenes de agrupaciones de almacenamiento secuenciales reutilizados.

Ejemplo: Visualizar información histórica de volúmenes de un volumen de agrupación de almacenamiento

Visualizar información histórica de volúmenes de un volumen de agrupación de almacenamiento almacenado en la base de datos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos. Emita el mandato:

```
query volhistory type=stgnew
```

```

Fecha/hora: 02/25/2011 18:28:06
Tipo volumen: STGNEW
Serie copia seguridad:
Operación copia seguridad:
  Sec. volumen:
Clase dispositivo: FILE
Nombre volumen: /adsmfct/server/prvoll
Ubicación volumen:
Mandato:
ID superior copia de seguridad base de datos:
ID inferior copia de seguridad base de datos:
Posición de reposo de copia de seguridad de base de datos:
  HLA copia de seguridad base de datos:
  LLA de copia de seguridad base de datos:
Bytes de datos totales de copia seguridad base de datos (MB):
Bytes de registro totales de copia seguridad base de datos:
Número de bloque superior de copia de seguridad base de datos:
Número de bloque inferior de copia de seguridad base de datos:

```

ID de corriente de copia de seguridad de base de
datos:
Secuencia de volumen de copia de seguridad de base de datos para corriente:

Nota: El archivo histórico de volúmenes contendrá campos adicionales que no aparecen en la salida de la consulta. Estos campos son específicos del soporte de copia de seguridad y restauración de base de datos. No son para que los utilicen o modifiquen los administradores de IBM Spectrum Protect. Los campos aparecerán entre corchetes con un mensaje que indica que son sólo para uso interno de IBM Spectrum Protect y que no deben ser modificados.

Ejemplo: la información histórica de volúmenes de visualización para un volumen de copia de seguridad de base de datos

Visualizar información histórica de volúmenes de un volumen de copia de seguridad de base de datos almacenado en la base de datos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos. Emita el mandato:

```
query volhistory type=dbb
```

```
                Fecha/hora: 02/25/2011 18:28:06
                Tipo volumen: BACKUPFULL
                Serie copia seguridad: 176
                Operación copia seguridad: 0
                Sec. volumen: 0
                Clase dispositivo: FILE
                Nombre volumen: /adsmfct/server/prv011
                Ubicación volumen:
                Mandato:
                ID superior copia de seguridad base de datos: 0
                ID inferior copia de seguridad base de datos: 0
                Posición inicial de copia de seguridad base de datos: 0
                HLA copia de seguridad base de datos:
                LLA de copia de seguridad base de datos:
                Bytes de datos totales de copia seguridad base de datos (MB): 0
                Bytes de registro totales de copia seguridad base de datos (MB): 0
                Número de bloque superior de copia de seguridad base de
datos: 0
                Número de bloque inferior de copia de seguridad base de
datos: 0
                ID de corriente de copia de seguridad de base de datos: 1
                Secuencia de volumen de copia de seguridad de base de datos para
corriente: 10.001
```

Nota: El archivo histórico de volúmenes contendrá campos adicionales que no aparecen en la salida de la consulta. Estos campos son específicos del soporte de copia de seguridad y restauración de base de datos. No son para que los utilicen o modifiquen los administradores de IBM Spectrum Protect. Los campos aparecerán entre corchetes con un mensaje que indica que son sólo para uso interno de IBM Spectrum Protect y que no deben ser modificados.

Descripciones de los campos

Fecha/Hora

La fecha y la hora de la creación del volumen.

Volume Type

El tipo del volumen:

BACKUPFULL

Volumen de copia de seguridad de base de datos completa.

BACKUPINCR

Volumen de copia de seguridad de base de datos incremental.

BACKUPSET

Volumen de juego de copias de seguridad de cliente.

DBSNAPSHOT

Volumen de copia de seguridad de instantánea de base de datos.

EXPORT

Exportar volumen.

REMOTE

Volumen que se utiliza en el cliente de biblioteca, que es el servidor de IBM Spectrum Protect que se ha especificado en el campo Ubicación del volumen. Consulte el histórico de volúmenes del servidor que es el cliente de biblioteca para obtener información detallada acerca de cómo se ha utilizado el volumen.

RPFIL

Volumen de objeto de archivo del plan de recuperación dándose por supuesto copias de seguridad de base de datos incrementales y completas.

RPFSnapshot

Volumen de objeto de archivo del plan de recuperación que se ha creado dándose por supuesto copias de seguridad de instantánea de base de datos.

STGDELETE

Volumen de agrupación de almacenamiento de acceso secuencial suprimido.

STGNEW

Volumen de agrupación de almacenamiento de acceso secuencial agregado.

STGREUSE

Volumen de agrupación de almacenamiento de acceso secuencial reutilizado.

Backup Series

El valor de este campo depende del tipo de volumen:

- Para los tipos de volumen BACKUPFULL o BACKUPINCR: el identificador de la serie de copia de seguridad.
- Para el tipo de volumen DBSNAPSHOT: el identificador de la serie de copia de seguridad que está asociado a la entrada DBSNAPSHOT.
- Para el tipo de volumen RPFIL: el identificador de la serie de copia de seguridad que está asociado a la entrada RPFIL.
- Para el tipo de volumen RPFSNAPSHOT: el identificador de la serie de copia de seguridad que está asociado a la entrada RPFSNAPSHOT.
- En tipos de volumen BACKUPSET este campo está en blanco.
- Para todos los demás tipos de volumen: siempre 0.

Una serie de copia de seguridad es un copia de seguridad completa y todas las copias de seguridad incrementales que se aplican a esa copia de seguridad completa. Otra serie empieza con la siguiente copia de seguridad completa de la base de datos.

Backup Operation

Para los tipos de volumen BACKUPFULL o BACKUPINCR: el número de operación de este volumen de copia de seguridad dentro de la serie de copia de seguridad. La copia de seguridad completa en una serie de copia de seguridad es la operación 0. La primera copia de seguridad incremental para dicha copia de seguridad completa es la operación 1, la segunda copia de seguridad incremental es la operación 2, y así sucesivamente.

Para los tipos de volumen DBSNAPSHOT: el número de operación de este volumen DBSNAPSHOT dentro de la serie DBSNAPSHOT.

Para todos los demás tipos de volumen: siempre 0.

Este campo está en blanco cuando el tipo de volumen es BACKUPSET.

Volume Seq

La secuencia o posición del volumen dentro de la serie de copia de seguridad.

- Para los tipos de volumen BACKUPFULL o BACKUPINCR: la secuencia, o posición, del volumen dentro de la serie de copia de seguridad. La secuencia de volumen 1 identifica el primer volumen utilizado para la primera operación (una copia de seguridad completa), etc. Por ejemplo, si la copia de seguridad completa ocupa tres volúmenes, estos volúmenes se identifican como la secuencia de volúmenes 1, 2 y 3. El primer volumen de la siguiente operación (la primera copia de seguridad incremental) es la secuencia de volumen 4.
- Para los tipos de volumen BACKUPSET: la secuencia, o posición, del volumen dentro de la serie de BACKUPSET.
- Para los tipos de volumen DBSNAPSHOT: la secuencia, o posición, del volumen dentro de la serie de DBSNAPSHOT. La secuencia de volumen 1 identifica el primer volumen utilizado para la primera operación DBSNAPSHOT, y así sucesivamente.
- Para los tipos de volumen EXPORT: el número de secuencia del volumen al utilizarlo para exportar los datos.
- Para los tipos de volumen RPFIL: el valor de este campo siempre es uno (1).
- Para todos los demás tipos de volumen: siempre 0.

Device Class

El nombre de la clase de dispositivo asociado a este volumen.

Volume Name

El nombre del volumen.

Volume Location

La ubicación del volumen. Esta información sólo está disponible para los siguientes tipos de volúmenes:

- BACKUPFULL
- BACKUPINCR
- EXPORT
- REMOTE

- RPFILe

Para el tipo de volumen REMOTE, este campo de ubicación es el nombre de servidor del cliente de biblioteca que es el propietario de este volumen.

Para el tipo de volumen RPFILe, este campo de ubicación es el nombre de servidor que se ha definido en la definición de clase de dispositivo que el mandato PREPARE utiliza cuando se especifica el parámetro DEVCLASS.

Mandato

Cuando el tipo de volumen es EXPORT o BACKUPSET y el número de secuencia del volumen es 1 (por ejemplo, el primer volumen), este campo muestra el mandato que se utilizó para generar el volumen. Si EXPORT o BACKUPSET están presentes en más de un volumen, el mandato visualiza el primer volumen, pero no visualiza ninguno de los demás volúmenes.

Para los tipos de volúmenes distintos de EXPORT o BACKUPSET, este campo está en blanco.

Consejo: Los campos siguientes no los utilizan los servidores de IBM Spectrum Protect que son de la versión 6.3 o posteriores. Sin embargo, los campos se visualizan con fines de compatibilidad con releases anteriores.

- ID superior de copia de seguridad base de datos
- ID inferior copia de seguridad base de datos
- Posición inicial de copia de seguridad base de datos
- HLA copia de seguridad base de datos
- LLA copia de seguridad base de datos
- Bytes de datos totales de copia seguridad base de datos (MB)
- Bytes de registro totales de copia seguridad base de datos (MB)
- Número de bloque superior de copia de seguridad base de datos
- Número de bloque inferior de copia de seguridad base de datos

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY VOLHISTORY

Mandato	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFILe	Muestra información sobre archivos del plan de recuperación.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)

Utilice este mandato para visualizar información acerca de uno o varios volúmenes de agrupación de almacenamiento.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

>>-Query Volume .-*-----+----->
                   +-nombre_volumen-'
>+-----+-----+----->
|           .-,-----+-----|
|           v          |
| '-ACCess-----+READWrite---+'
|           +-READOnly----+
|           +-UNAVailable-+

```


suprimieron, pero que todavía contienen datos descartados que están a la espera de ser destruidos. Después de destruir los datos, el volumen se suprimirá físicamente.

FILLING

Se visualizan los volúmenes de acceso secuencial en los que el servidor ha grabado pero que todavía no ha llenado hasta su capacidad.

FULL

Se visualizan los volúmenes de acceso secuencial que el servidor ha llenado.

STGPool

Especifica la agrupación de almacenamiento que se incluye en la consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de agrupación de almacenamiento, se incluirán en la consulta todas las agrupaciones de almacenamiento.

DEVclass

Especifica la clase de dispositivo que se incluye en la consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de clase de dispositivo, se incluirán en la consulta todos los dispositivos.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.


 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: obtener una lista de todos los volúmenes de agrupación de almacenamiento de archivo

Visualizar información acerca de todos los volúmenes de agrupación de almacenamiento que tengan el nombre de clase de dispositivo FILE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume devclass=file
```

Nombre volumen	Nombre agrupación almacenam.	Nombre clase	Capacidad estimada	% Util	Estado volumen
/FCT/SERVER/COV011	COPYSTG	FILE	0.0 M	0.0	Pend.
/FCT/SERVER/COV012	COPYSTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/COV013	COPYSTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/PRV011	PRIMESTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/PRV012	PRIMESTG	FILE	0.0 M	0.0	Vacío

 Sistemas operativos Windows

Ejemplo: obtener una lista de todos los volúmenes de agrupación de almacenamiento que tienen el mismo prefijo

Visualizar información acerca de todos los volúmenes de agrupación de almacenamiento que tengan como prefijo el nombre ATF. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume atf*
```

Nombre volumen	Nombre agrupación almacenam.	Nombre clase	Capacidad estimada	% Util	Estado volumen
ATF001	8MMPOOL	8MMTAPE	4.8 G	18.2	Llenando
ATF002	8MMPOOL	8MMTAPE	4.8 G	18.2	Llenando

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

Visualizar detalles sobre el volumen de agrupación de almacenamiento denominado /fct/server/cov011. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume cov011 format=detailed
```

```

Nombre volumen: /FCT/SERVER/COV011
Nombre agrupación almacenamiento: COPYSTG
Nombre de clase de dispositivo: DISK
Capacidad estimada: 10,0 M
Capacidad de escala aplicada:
  % Util: 6,7
Estado volumen: Activado
  Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 3,2
  ¿Volumen reutilizable?: Sí
  ¿Con error?: No
Número caras grabables: 1
Número montajes: 11
  Número pases grabación: 1
Fecha aprox. última grabación: 04/14/1998 16:17:26
Fecha aprox. última lectura: 04/01/1998 13:26:18
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
El volumen es MVS con posibilidad
  fuera de la LAN: No
Última actualización por (administrador): COLLIN
Fecha/hora última actualización: 05/01/1998 14:07:27
Empezar período de reclamación:
Finalizar período de reclamación:
Bloque lógico protegido:
Gestor de claves de cifrado de unidad:

```

 Sistemas operativos Windows

Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

Visualizar detalles sobre el volumen de agrupación de almacenamiento WPDV00. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume wpdv00 format=detailed
```

```

Nombre volumen: WPDV00
Nombre agrupación almacenamiento: TAPEPOOL
Nombre clase dispositivo: TAPE
Capacidad estimada: 5,8 M
Capacidad de escala aplicada:
  % Util: 0,1
Estado volumen: Activado
  Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 3,2
  ¿Volumen reutilizable?: Sí
  ¿Con error?: No
Número caras grabables: 1
Número montajes: 11
  Número pases grabación: 1
Fecha aprox. última grabación: 04/14/1998 16:17:26
Fecha aprox. última lectura: 04/01/1998 13:26:18
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
El volumen es MVS con posibilidad
  fuera de la LAN: No
Última actualización por (administrador): COLLIN
Fecha/hora última actualización: 05/01/1998 14:07:27
Empezar período de reclamación:
Finalizar período de reclamación:
Bloque lógico protegido:
Gestor de claves de cifrado de unidad:

```

Ejemplo: visualizar información detallada acerca de un volumen de agrupación de almacenamiento que tiene una clase de dispositivo específica

Muestra detalles sobre un volumen en una agrupación de almacenamiento con un nombre de clase de dispositivo FILECLASS. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume devclass=fileclass format=detailed
```

```

  Sistemas operativos WindowsNombre volumen: Z:\WORM_CFS\0000000E.BFS
  Sistemas operativos AIXSistemas operativos LinuxNombre volumen:
/WORM_FILESYS/0000000E.BFS
  Nombre agrupación almacenamiento: FILEPOOL
  Nombre de clase de dispositivo: FILECLASS
  Capacidad estimada: 2 G
  Capacidad de escala aplicada:
    % Util: 0,0
  Estado volumen: Llenando
  Acceso: Lectura/Grabación
  Porcentaje de espacio reclamable: 0,0
  ¿Volumen reutilizable?: Sí
  ¿Con error?: No
  Número caras grabables: 1
  Número de montajes: 1
  Número pases grabación: 1
  Fecha aprox. última grabación: 03/22/2004 15:23:46
  Fecha aprox. última lectura: 03/22/2004 15:23:46
  Fecha en que pasó a pendiente:
  Número errores grabación: 0
  Número errores lectura: 0
  Ubicación volumen:
  El volumen es MVS con posibilidad
                                fuera de la LAN: No
  Última actualización por (administrador):
  Fecha/hora última actualización: 03/22/2004 15:23:46
  Empezar período de reclamación: 03/22/2005
  Finalizar período de reclamación: 04/22/2005
  Bloque lógico protegido:
  Gestor de claves de cifrado de unidad:
```

Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

Visualizar detalles sobre un volumen de agrupación de almacenamiento que se denomina 000642. El volumen está en una agrupación de almacenamiento que está asociada con una clase de dispositivo 3592. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume 000642 format=detailed
```

```

  Nombre volumen: 000642
  Nombre agrupación almacenamiento: 3592POOL
  Nombre clase dispositivo: 3592CLASS
  Capacidad estimada: 2 G
  Capacidad de escala aplicada:
    % Util: 0,0
  Estado volumen: Llenando
  Acceso: Lectura/Grabación
  Porcentaje de espacio reclamable: 0,0
  ¿Volumen reutilizable?: Sí
  ¿Con error?: No
  Número caras grabables: 1
  Número de montajes: 1
  Número pases grabación: 1
  Fecha aprox. última grabación: 03/22/2004 15:23:46
  Fecha aprox. última lectura: 03/22/2004 15:23:46
  Fecha en que pasó a pendiente:
  Número errores grabación: 0
  Número errores lectura: 0
  Ubicación volumen:
  El volumen es MVS con posibilidad
                                fuera de la LAN: No
  Última actualización por (administrador):
  Fecha/hora última actualización: 03/22/2004 15:23:46
  Empezar período de reclamación: 03/22/2005
  Finalizar período de reclamación: 04/22/2005
  Bloque lógico protegido: Sí
  Drive Encryption Key Manager: IBM Spectrum Protect
```

Descripciones de los campos

Nombre de volumen

El nombre del volumen de agrupación de almacenamiento.

Nombre de la agrupación de almacenamiento
La agrupación de almacenamiento en la que está definido el volumen.

Nombre clase dispositivo
La clase de dispositivo que se asigna a la agrupación de almacenamiento.

Capacidad estimada
La capacidad estimada del volumen, en megabytes (M), gigabytes (G) o terabytes (T).

Para dispositivos DISK, este valor es la capacidad del volumen.

Para dispositivos de acceso secuencial, este valor es un cálculo del espacio total disponible en el volumen, que se basa en la clase de dispositivo.

Capacidad de escala aplicada
El porcentaje de la capacidad a la que se ha escalado un volumen. Por ejemplo, un valor de 20 para un volumen cuya capacidad máxima es de 300 GB indica que el volumen sólo puede almacenar 20 un por ciento de 300 GB o 60 GB. Este atributo solamente se aplica a los dispositivos IBM® 3592.

Pct. util
Un cálculo de la utilización del volumen. La utilización incluye todo el espacio que ocupan ambos archivos y agregados, incluido el espacio vacío dentro de agregados.

Para volúmenes DISK, la utilización también incluye el espacio que ocupan los datos almacenados en caché.

Estado volumen
El estado del volumen.

Acceso
Si el volumen está disponible para el servidor.

Porcentaje de Espacio reclamable (sólo volúmenes de acceso secuencial)
La cantidad de espacio de este volumen que puede reclamarse porque los datos han caducado o se han suprimido. Este valor se compara con el umbral de reclamación de la agrupación de almacenamiento para determinar si es necesaria la reclamación. El espacio reclamable incluye el espacio vacío en las agregaciones.

Cuando se determina qué volúmenes se reclaman en una agrupación de almacenamiento, el servidor determina primero el umbral de reclamación. El umbral de reclamación viene indicado por el valor del parámetro THRESHOLD en el mandato RECLAIM STGPOOL o, si no se ha especificado dicho valor, el valor del parámetro RECLAIM en una definición de agrupación de almacenamiento. A continuación, el servidor examina el porcentaje de espacio reclamable de cada volumen en la agrupación de almacenamiento. Si el porcentaje de espacio reclamable que hay en un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento, el volumen es candidato para la reclamación.

Por ejemplo, supongamos que la agrupación de almacenamiento FILEPOOL tiene un umbral de reclamación del 70 por ciento. Este valor indica que el servidor puede reclamar cualquier volumen en la agrupación de almacenamiento que tenga un porcentaje de espacio reclamable mayor del 70 por ciento. La agrupación de almacenamiento tiene tres volúmenes:

- FILEVOL1 con el 65 por ciento de espacio reclamable
- FILEVOL2 con el 80 por ciento de espacio reclamable
- FILEVOL3 con el 95 por ciento de espacio reclamable

Cuando empieza la reclamación, el servidor compara el porcentaje de espacio reclamable de cada volumen con el umbral de reclamación del 70 por ciento. En este ejemplo, FILEVOL2 y FILEVOL3 son candidatos para la reclamación porque sus porcentajes de espacio reclamable son mayores que el 70 por ciento.

Para volúmenes que pertenecen una agrupación de almacenamiento de SnapLock, el valor se visualiza pero no se utiliza.

¿Volumen reutilizable? (sólo volúmenes de acceso secuencial)
Si este volumen se puede reutilizar cuando el volumen se vacía.

¿Con error?
Si el volumen está en un estado de error. El servidor no puede grabar en volúmenes que tienen un estado de error.

Número caras grabables
Esta información está reservada para IBM Spectrum Protect.

Número montajes
El número de veces que el servidor abre el volumen para su uso. El número de veces que el servidor ha abierto el volumen no siempre coincide con que el número de veces que se ha montado físicamente el volumen en una unidad. Una vez montado físicamente un volumen, el servidor puede abrir el mismo volumen varias veces para distintas operaciones, como por ejemplo para distintas sesiones de copia de seguridad de cliente.

Número de pases de grabación (sólo volúmenes de acceso secuencial)
El número de veces que se ha grabado en el volumen desde el principio al final.

Fecha aprox. última grabación

- La fecha aproximada en que se ha grabado el volumen por última vez.
- Fecha aprox. última lectura
 - La fecha aproximada en que se ha leído el volumen por última vez.
- Fecha en que pasó a pendiente
 - La fecha en que el estado del volumen se ha modificado a pendiente.
- Número errores grabación
 - El número de errores de grabación que se han producido en el volumen.
- Número errores lectura
 - El número de errores de lectura que se han producido en el volumen.
- Ubicación del volumen
 - La ubicación del volumen.
- El volumen es MVS con posibilidad fuera de la LAN
 - Si el volumen es un volumen con posibilidad fuera de la LAN. Un volumen con posibilidad fuera de la LAN es aquél que ha definido y ha utilizado (como mínimo una vez) el servidor del gestor de datos de IBM Spectrum Protect z/OS.
- Última actualización por (administrador)
 - El administrador que ha definido o que ha actualizado más recientemente el volumen.
- Fecha/hora última actualización
 - El momento en que se ha definido o actualizado más recientemente el volumen.
- Empezar período de reclamación

Representa la fecha después de la cual el servidor inicia la reclamación de este volumen, pero que no debe ser posterior a la fecha que representa el fin del período de reclamación. Si, cuando empieza el periodo de reclamación, hay archivos en el volumen que no han caducado, estos se trasladan a un nuevo volumen WORM durante el proceso de reclamación. Este campo muestra una fecha sólo si este volumen está en una agrupación de almacenamiento para la que el valor del parámetro RECLAMATIONTYPE es SNAPLOCK.

Si se almacena más de un archivo en el mismo volumen, el inicio del período de reclamación del volumen se basa en la fecha del archivo más reciente. Para los volúmenes SnapLock, el parámetro RETVer del mandato DEFINE COPYGROUP determina durante cuánto tiempo se almacenará una copia archivada. Si RETVer se define en 100 días, el período de reclamación del volumen se iniciará 100 días después de que el primer archivo se almacene en él. Si se almacena un segundo archivo en el mismo volumen, la fecha de inicio de la reclamación se ajustará a 100 días después de que se almacene el nuevo archivo. Si el valor de RETVer se modifica una vez que el primer archivo ya se ha almacenado, se aplicará la última fecha de reclamación para todos los archivos del volumen. Por ejemplo, supongamos que RETVer se define en 100 para un archivo inicial, pero luego se cambia a 50. Si se almacena un segundo archivo en el volumen tres días después del primero, el período de reclamación no empezará hasta pasados 100 días desde el almacenamiento del primer archivo.
- Finalizar período de reclamación

Representa la fecha en la que IBM Spectrum Protect debe completar el proceso de reclamación de este volumen para garantizar la protección continuada de los datos. También representa el atributo de archivo físico Fecha de último acceso en el archivador NetApp, que impide que el archivo se suprima hasta después de esa fecha. Este campo muestra una fecha sólo si este volumen está en una agrupación de almacenamiento para la que el valor del parámetro RECLAMATIONTYPE es SNAPLOCK.
- Gestor de claves de cifrado de unidad

El gestor de claves de cifrado de unidad. Este campo se aplica sólo a volúmenes de una agrupación de almacenamiento que está asociada a un tipo de dispositivo de 3592, LTO o ECARTRIDGE.
- Bloque lógico protegido

Especifica si la protección de bloques lógicos está habilitada para el volumen. Puede utilizar la protección de bloques lógicos solamente con los siguientes tipos de unidades y medios:

 - IBM LTO5 y posterior
 - Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior
 - Unidades Oracle StorageTek T10000C y T10000D

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY VOLUME

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

Mandato	Descripción
VARY	Especifica si está disponible un volumen de disco para el servidor.

QUIT (finalizar la modalidad interactiva del cliente de administración)

Utilice este mandato para finalizar una sesión de cliente de administración en modalidad interactiva.

No puede utilizar el mandato QUIT desde el identificador de administración SERVER_CONSOLE ni desde las modalidades de consola, por lotes o de montaje del cliente de administración.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-QUIT-----<<
```

Parámetros

Ninguno.

Ejemplo: finalizar una sesión de cliente de administración interactiva

Finalizar una sesión del cliente de administración en modalidad interactiva.

```
quit
```

Mandatos relacionados

Ninguno.

RECLAIM STGPOOL (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)

Utilice este mandato para reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial. La reclamación no traslada las versiones inactivas de los datos de copia de seguridad de los volúmenes en las agrupaciones de datos activos.

Este mandato no se puede utilizar para los tipos siguientes de agrupaciones de almacenamiento:

- Agrupaciones de almacenamiento de copia de contenedor. El espacio de estas agrupaciones de almacenamiento se reclama como parte del proceso realizado por mandatos PROTECT STGPOOL.
- Agrupaciones de almacenamiento con uno de los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
- Agrupaciones de almacenamiento que utilizan una clase de dispositivo de CENTERA.
- Agrupaciones de almacenamiento que utilizan dispositivos WORM (Grabar una vez leer varias). La reclamación no es necesaria porque los volúmenes WORM no son reutilizables, pero puede ejecutar la reclamación para consolidar los datos en menos volúmenes.

Utilice este mandato sólo si no va a utilizar la reclamación automática para la agrupación de almacenamiento. Este mandato acepta los valores de los atributos RECLAIMPROCESS y RECLAIMSTGPOOL de la definición de agrupación de almacenamiento. Este mandato también acepta los valores de los parámetros OFFSITERECLAIMLIMIT y RECLAIM de la definición de agrupación de almacenamiento, si no los han alterado temporalmente los parámetros de mandato OFFSITERECLAIMLIMIT y THRESHOLD.

Consejos:

- Al emitir este mandato se eliminan los datos duplicados de una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia o una agrupación de datos activos configurada para la deduplicación de datos.

- Cuando se utiliza este mandato para restaurar objetos deduplicados a la misma agrupación de almacenamiento, los bloques de datos duplicados se sustituyen por referencias a las extensiones deduplicadas.

Para las agrupaciones de almacenamiento definidas con RECLAMATIONTYPE=SNAPLOCK, este mandato también suprime los volúmenes WORM FILE vacíos que exceden su periodo de reclamación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado para la agrupación de almacenamiento que se está reclamando y la agrupación de almacenamiento de reclamación, si procede.

Sintaxis

```
>>-RECLaim STGpool--nombre_agrupación----->
>--+-----+--+-----+----->
  '-THreshold---número-'  '-Duration---minutos-'

  .-Wait---No-----.
>--+-----+--+-----+----->
  '-Wait---+No--+-'
                '-Yes-'

>--+-----+-----><
  '-OFFSITERECLAIMLimit---número_de_volúmenes-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento cuyos volúmenes se reclamarán.

DURATION

Especifica el número máximo de minutos que se ejecuta la migración antes de que se cancele automáticamente. Puede especificar un número de 1 a 9999. Este parámetro es opcional.

Después de transcurrir el número de minutos especificado, la próxima vez que el servidor verifique el proceso de reclamación lo detendrá. El servidor comprueba el proceso de reclamación cuando monta otro volumen elegible de la agrupación de almacenamiento que se está reclamando. El servidor también comprueba el proceso de reclamación cuando el servidor empieza a reclamar un nuevo lote de archivos del volumen que está montado actualmente. Como consecuencia, la reclamación puede ejecutarse durante más tiempo que el valor que especifique para este parámetro.

Hasta que el servidor no verifique el proceso de reclamación, no existe ninguna indicación de que haya caducado el período de duración. Cuando el servidor detiene el proceso de reclamación, emite el mensaje ANR4927W: Se ha terminado la reclamación para el volumen xxx - se ha sobrepasado la duración.

Si no especifica este parámetro, el proceso se detendrá únicamente cuando no haya más volúmenes que satisfagan el umbral.

Si especifica un valor de duración para la reclamación de una agrupación de almacenamiento de copia con volúmenes fuera del local, puede provocar que la reclamación finalice antes de que se haya reclamado cualquier volumen. En la mayoría de situaciones al iniciar la reclamación de una agrupación de almacenamiento con volúmenes fuera del local, se recomienda limitar el número de volúmenes fuera del que deben reclamarse en lugar de limitar la duración. Para obtener información adicional, consulte el parámetro OFFSITERECLAIMLIMIT.

THRESHOLD

Especifica el porcentaje de espacio reclamable en un volumen que permite seleccionarlo para la reclamación. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos. El espacio reclamable también incluye el espacio no utilizado.

Puede especificar un número del 1 al 99. Este parámetro es opcional. Si no se especifica, se utiliza el atributo RECLAIM de la definición de agrupación de almacenamiento.

Para determinar el porcentaje de espacio reclamable de un volumen, emita el mandato QUERY VOLUME y especifique FORMAT=DETAILED. El valor en el campo Porcentaje de espacio reclamable es el porcentaje de espacio reclamable del volumen.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de destino.

OFFSITERECLAIMLimit

Especifica el número máximo de volúmenes de agrupaciones de almacenamiento fuera del local que el servidor intenta reclamar. Este parámetro sólo es válido para las agrupaciones de almacenamiento de copia. Puede especificar un número del 0 al 99999. Este parámetro es opcional. Si no se especifica, se utiliza el atributo OFFSITERECLAIMLIMIT de la definición de agrupación de almacenamiento.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Si cancela este proceso, pueden haberse trasladado ya algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. La operación debe estar terminada para poder continuar con otras tareas. Cuando finaliza la operación, se muestran mensajes de salida en el cliente de administración. Los mensajes también se visualizan en las anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial

Reclamar volúmenes de la agrupación de almacenamiento denominada TAPEPOOL. Especificar que la reclamación finaliza lo antes posible pasados 60 minutos.

```
reclaim stgpool tapepool duration=60
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RECLAIM STGPOOL

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
MIGRATE STGPOOL	Migra archivos de una agrupación de almacenamiento primaria a la agrupación de almacenamiento siguiente en la jerarquía.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.

RECONCILE VOLUMES (Reconciliar diferencias en definiciones de volúmenes virtuales)

Emita este mandato desde el servidor de origen para reconciliar las diferencias que hay entre las definiciones de volúmenes virtuales del servidor de origen y las copias archivadas del servidor de destino. IBM Spectrum Protect localiza todos los volúmenes de la clase de dispositivo especificada del servidor de origen y todas las copias archivadas correspondientes del servidor de destino. El inventario del servidor de destino también se compara con la definición local de los volúmenes virtuales para ver si existen incoherencias.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

.&-----
>>-REConcile Volumes--+----->
      '-nombre_clase_dispositivo-'

.-Fix---No-----
>--+-----<
      '-Fix---+No---+'
          '-Yes-'

```

Parámetros

nombre_clase_dispositivo

Especifica el nombre de la clase de dispositivo de los volúmenes virtuales. Si no especifica un nombre, IBM Spectrum Protect reconcilia todos los volúmenes virtuales. Este parámetro es opcional.

FIX

Especifica si IBM Spectrum Protect intenta corregir todas las incoherencias identificadas. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que IBM Spectrum Protect no arregla ninguna incoherencia.

Yes

Especifica que IBM Spectrum Protect hace las correcciones siguientes:

- IBM Spectrum Protect marca como no disponibles los volúmenes de agrupación de almacenamiento del servidor de origen que no se pueden localizar en el servidor de destino. Los volúmenes que sólo se encuentran en el archivo histórico de volúmenes, como, por ejemplo, los volúmenes de importación y exportación y las copias de seguridad de base de datos, se registrarán como incoherentes.
- Las copias archivadas del servidor de destino que no se correspondan con ningún volumen virtual en el servidor de origen se marcan para suprimirlas del servidor de destino.

La tabla siguiente muestra los detalles de las acciones que se ejecutan:

FIX=	En el servidor origen	En el servidor destino	Acción
NO	Existen volúmenes	No existen archivos	Informar sobre error
		Los archivos existen pero están marcados para supresión	
		Existen archivos activos pero los atributos no coinciden	
	Los volúmenes no existen	Existen volúmenes activos	Informar sobre error
Los archivos existen pero están marcados para supresión		Ninguno	
YES	Existen volúmenes	No existen archivos	Informar sobre error Volúmenes de agrupación de almacenamiento: Marcados como no disponibles
		Los archivos existen pero están marcados para supresión	Informar sobre error Volúmenes de agrupación de almacenamiento: Si los atributos coinciden, marcar los archivos del servidor de destino como activos de nuevo, marcar los volúmenes del servidor de origen como no disponibles y recomendar que se ejecute un mandato AUDIT VOLUME para verificar los datos. Si los atributos no coinciden, marcar los volúmenes como no disponibles.
		Existen archivos activos pero los atributos no coinciden	Informar sobre error Volúmenes de agrupación de almacenamiento: Marcar como no disponibles y recomendar que se ejecute un mandato AUDIT VOLUME para verificar los datos.

FIX=	En el servidor origen	En el servidor destino	Acción
	Los volúmenes no existen	Existen volúmenes activos	Marcar archivos para supresión en el servidor de destino.
		Los archivos existen pero están marcados para supresión	Ninguno

Ejemplo: reconciliar las diferencias en las definiciones de volumen virtual

Reconciliar las diferencias que hay entre todas las definiciones de volúmenes virtuales del servidor de origen y las copias archivadas den el servidor de destino para corregir las incoherencias.

```
reconcile volumes remotel fix=yes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RECONCILE VOLUMES

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE SERVER	Suprime la definición de un servidor.
QUERY SERVER	Muestra información sobre servidores.
UPDATE SERVER	Actualiza la información sobre un servidor.

Mandatos REGISTER

Utilice los mandatos REGISTER para definir o agregar objetos para IBM Spectrum Protect.

- REGISTER ADMIN (Registrar un ID de administrador)
- REGISTER LICENSE (Registrar una nueva licencia)
- REGISTER NODE (Inscribir un nodo)

REGISTER ADMIN (Registrar un ID de administrador)

Utilice este mandato para agregar un administrador al servidor. Una vez registrado, el administrador puede emitir un conjunto de mandatos limitado, incluidos todos los mandatos de consulta. Para proporcionar privilegios adicionales, utilice el mandato GRANT AUTHORITY.

Clase de privilegio

Para emitir este mandato, debe tener privilegios del sistema.

Al registrar un administrador con el mismo nombre que un nodo existente, tenga en cuenta el método de autenticación de administrador y el valor de SSLREQUIRED. Cualquier nodo que tiene el mismo nombre que el administrador que se está registrando hereda esos valores.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- No especifique un ID de usuario de administración que coincida con un nombre de nodo. Si el ID de usuario de administración coincide con el nombre del nodo, podría darse un comportamiento imprevisto debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

Sintaxis

```

>>-REGister Admin--nombre_admin--+-----+----->
                                     '-password-'

>+-----+-----+-----+----->
| (1) | | '-CONTACT--==--texto-'
|-----PASSExp-----días-'

.-FORCEPwreset-----No-----
>+-----+-----+-----+----->
| '-FORCEPwreset-----+No--+-'
|                               '-Yes-'

>+-----+-----+-----+----->
| '-EMAILAddress-----ID_usuario@nodo-'

(2)
.------AUTHentication-----LOCAL-.
>+-----+-----+-----+----->
| '-AUTHentication-----+LOCAL+----'
|                               '-LDap--'

(3)
.-SSLrequired-----DEFAULT-----
>+-----+-----+-----+----->
| '-SSLrequired-----+Yes-----+--'
|                               +-No-----+
|                               '-DEFAULT-'

.-SESSIONSECurity-----TRANSitional-----
>+-----+-----+-----+----->
| '-SESSIONSECurity-----+STRict-----+-'
|                               '-TRANSitional-'

.-ALert-----No-----
>+-----+-----+-----+-----><
| '-ALert-----+Yes--+-'
|                               '-No--'

```

Notas:

1. El mandato PASSEXP no se aplica a los administradores que se autentican en un servidor de directorios LDAP.
2. El valor predeterminado puede cambiar si emitió el mandato SET DEFAULTAUTHENTICATION y especificó LDAP.
3. El parámetro SSLREQUIRED está en desuso.

Parámetros

nombre_admin (Necesario)

Especifica el nombre del administrador que se ha de registrar. La longitud máxima del nombre es de 64 caracteres.

No puede especificar NONE como nombre de administrador.

Si tiene previsto autenticar el ID de administrador con un servidor LDAP, asegúrese de que el ID de administrador no coincida con el nombre de cualquier nodo que se autentique con un servidor LDAP.

contraseña

Especifica la contraseña del administrador que se ha de registrar. La longitud máxima de la contraseña es de 64 caracteres.

Si autentica contraseñas localmente con el servidor IBM Spectrum Protect, debe especificar una contraseña. La contraseña no es sensible a las mayúsculas y minúsculas.

Si autentica contraseñas con un servidor LDAP (Lightweight Directory Access Protocol), no especifique una contraseña en el mandato REGISTER ADMIN.

PASSExp

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña en el rango de 0 – 9999 días. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, la contraseña se establecerá con el período de caducidad global de 90 días. Este parámetro no afecta a las contraseñas que se almacenan en un servidor de directorios LDAP.

CONTACT

Especifica información que identifica al administrador que se ha registrado. Este parámetro es opcional. La longitud máxima de esta serie es de 255 caracteres. La información de contacto debe estar encerrada entre comillas, si contiene espacios en blanco.

FORCEPwreset

Especifica si el administrador tiene que cambiar o restablecer la contraseña. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el administrador no necesita cambiar ni restablecer la contraseña al intentar conectarse al servidor.

Yes

Especifica que la contraseña del administrador caduca durante el próximo inicio de sesión. El cliente o el administrador deben cambiar o restablecer la contraseña en ese momento. Si no se especifica una contraseña, recibirá un mensaje de error.

Restricción: En el caso de los ID de usuarios administrativos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si especifica AUTHENTICATION=LDAP.

EMAILAddress

Especifica la dirección de correo electrónico de este administrador.

AUTHentication

Este parámetro especifica el método de autenticación para el ID de usuario administrador. Especifique uno de los siguientes valores: LDAP o LOCAL. El parámetro es opcional y toma el valor predeterminado LOCAL. El valor predeterminado se puede cambiar a LDAP si se utiliza el mandato SET DEFAULTAUTHENTICATION y especifica LDAP.

Local

Especifica que se está utilizando la base de datos del servidor IBM Spectrum Protect .

LDap

Especifica que el ID de usuario administrador autentica contraseñas con un servidor de directorio LDAP. Las contraseñas que se autentican con un servidor de directorios LDAP distinguen entre mayúsculas y minúsculas.

Consejo: No se necesita contraseña si registra un administrador y selecciona AUTHENTICATION=LDAP. Al iniciar la sesión, se le solicitará una contraseña.

SSLrequired (en desuso)

Especifica si el ID de usuario administrador debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect y el cliente de archivado y copia de seguridad. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red

Importante: A partir del software de IBM Spectrum Protect Versión 8.1.2 y del software de Tivoli Storage Manager Versión 7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

SESSIONSECurity

Especifica si el administrador debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el administrador. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el administrador. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el administrador pueda autenticarse en el servidor:

- Tanto el administrador como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el administrador para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el administrador.

Los administradores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

TRANSitional

Especifica que se aplicarán los valores de seguridad existentes para el administrador. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el administrador no cumple nunca los requisitos para el valor STRICT, el administrador continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un administrador cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de

TRANSITIONAL a STRICT. Después, el administrador ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el administrador se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un administrador que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como el direccionamiento de mandatos o la exportación entre servidores, cuando el administrador se autentica en el servidor IBM Spectrum Protect como administrador de otro servidor.

Alert

Especifica si las alertas se envían a una dirección de correo electrónico de los administradores.

Yes

Especifica que las alertas se envíen a la dirección de correo electrónico especificada de los administradores.

No

Especifica que las alertas no se envíen a la dirección de correo electrónico especificada de los administradores. Este es el valor predeterminado.

Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

Ejemplo: registrar un administrador

Definir un administrador, LARRY, con la contraseña PASSONE. Puede identificar a LARRY como personal de segundo turno, especificando esta información en el parámetro CONTACT. Emita el mandato:

```
register admin larry passone contact="segundo turno"
```

Ejemplo: registrar un ID de administrador y establecer el método de autenticación

Defina un ID de administrador para Harry de forma que Harry pueda autenticarse en un servidor LDAP. Emita el mandato:

```
register admin harry authentication=ldap
```

Ejemplo: registrar un administrador y forzar la seguridad de sesión estricta

Registre un administrador llamado Harry y exija que utilice la configuración de seguridad más estricta para autenticarse en el servidor. Emita el mandato:

```
register admin harry sessionsecurity=strict
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REGISTER ADMIN

Mandato	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE ADMIN	Suprime un administrador de la lista de administradores registrados.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.

Mandato	Descripción
UNLOCK ADMIN	Permite que un administrador bloqueado acceda a IBM Spectrum Protect.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

Tareas relacionadas:

Nombrar objetos de Tivoli Storage Manager

Referencia relacionada:

[Opción de cliente SSL](#)

REGISTER LICENSE (Registrar una nueva licencia)

Utilice este mandato para registrar licencias nuevas para componentes del servidor, incluyendo IBM Spectrum Protect (base), IBM Spectrum Protect Extended Edition y IBM Spectrum Protect para retención de datos.

Las licencias se almacenan en los archivos de certificados de inscripción. Los archivos de certificados de inscripción contienen información de licencias para el producto del servidor. El archivo NODELOCK conserva la información de licencias de la instalación. Su acuerdo de licencia determina qué puede utilizar con su licencia, aunque no pueda usar el mandato REGISTER LICENSE para registrar todos los componentes. Se espera que cumpla con el acuerdo de licencia y utilice sólo lo que ha adquirido. El uso del mandato REGISTER LICENSE implica que acepta los términos de licencia de su acuerdo de licencia.

Importante:

- Antes de proceder a la actualización de una versión anterior de IBM Spectrum Protect, debe suprimir el archivo NODELOCK o cambiarle el nombre.
- Para anular licencias, debe borrar el archivo NODELOCK en el directorio de instancia del servidor de la instalación y volver a registrar las licencias registradas previamente.
- No se pueden registrar licencias de IBM Spectrum Protect para correo, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect para ERP y IBM Spectrum Protect for Space Management.

Para generar un informe que pueda ayudarle a conocer los requisitos de licencia del sistema, ejecute el mandato QUERY PVUESTIMATE. El informe contiene estimaciones del número de dispositivos de cliente y los totales de PVU de los dispositivos de servidor. Las estimaciones no son vinculantes jurídicamente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REGister LICense--FILE--==--+-tsmbasic.lic+-----><
                                     +-tsmee.lic----+
                                     +-dataret.lic--+
                                     '-*.lic-----'
```

Parámetros

FILE

Especifica el nombre del archivo de certificados de inscripción que contiene la licencia que se ha de registrar. La especificación puede contener un carácter comodín (*). Especifique el nombre de archivo completo o un carácter comodín en lugar del nombre de archivo. Los nombres de archivos son sensibles a las mayúsculas/minúsculas. Se pueden utilizar los siguientes valores:

tsmbasic.lic

Para obtener la licencia de IBM Spectrum Protect base.

tsmee.lic

Para obtener la licencia de IBM Spectrum Protect Extended Edition. Esto incluye el gestor de recuperación ante siniestro, bibliotecas de gran tamaño y NDMP.

dataret.lic

Para obtener la licencia de IBM Spectrum Protect para retención de datos. Es necesaria para activar la protección de retención de datos y también la suspensión de caducidad y supresión (retención de supresión).

*.lic

Para obtener la licencia de todas las licencias de IBM Spectrum Protect para componentes del servidor.

Ejemplo: registrar una licencia

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REGISTER LICENSE

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY PVUESTIMATE	Muestra las estimaciones de las unidades de valor de procesador.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.

REGISTER NODE (Inscribir un nodo)

Utilice este mandato para inscribir un nodo en el servidor.

Este mandato puede crear un ID de usuario de administración con autorización de propietario de cliente sobre el nodo. Puede utilizar este identificador de usuario de administración para acceder al cliente de copia de seguridad/archivado de web desde ubicaciones remotas mediante un navegador web.

Consejo:

- En versiones anteriores del producto, el mandato REGISTER NODE creaba automáticamente un ID de usuario de administración cuyo nombre coincidía con el nombre de nodo. A partir de IBM Spectrum Protect V8.1, el mandato REGISTER NODE no crea automáticamente un ID de usuario de administración que coincide con el nombre del nodo.
- Si tiene previsto utilizar la opción sin LAN con este nodo, debe registrar un ID administrativo que coincida con el nombre de nodo. Para registrar el ID administrativo, utilice el parámetro USERID o registre manualmente el administrador y otórguele autoridad de propietario para el nodo.

Si un cliente necesita un dominio de políticas distinto de STANDARD, deberá inscribir el nodo cliente con este mandato o actualizar el nodo inscrito.

Requisito: Cuando establece `sslrequired=serveronly` en un mandato REGISTER NODE, el valor SSLREQUIRED vuelve a ser YES. Para utilizar una sesión que no es SSL con un agente de almacenamiento, cambie el nombre al administrador por el nombre idéntico emitiendo el mandato RENAME ADMIN .

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión. Cuando se registra o actualiza un nodo, puede especificar si los archivos dañados en el nodo pueden recuperarse de un servidor de réplica. Los archivos sólo se pueden recuperar si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores de los parámetros a la recuperación de archivos dañados y replicados.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	No especificado	NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-REGister Node--nombre_nodo--+-+-----+----->
                                     '-password-'
                                     .-USerid----NONE-----
>+-----+-----+-----+----->
| (1) | '-USerid----+NONE-----+'
|-----PASSExp----días-' | '-id_usuario-'
                                     .-Dmain----STANDARD-----
>+-----+-----+-----+----->
'-CONTACT----texto-' '-Dmain-----nombre_dominio--'
                                     .-COMPression----Client----- .-ARCHDElete----Yes-----
>+-----+-----+-----+----->
'-COMPression----+Client+-' '-ARCHDElete----+Yes+-'
      +-Yes-----+           '-No--'
      '-No-----'
                                     .-BACKDElete----No-----
>+-----+-----+-----+----->
'-BACKDElete----+No--+-'
      '-Yes-'
                                     .-CLOptset----option_set_name-'
                                     .-FORCEPwreset----No----- .-Type----Client-----
>+-----+-----+-----+----->
'-FORCEPwreset----+No--+-' '-Type----+Client----+'

```

```

          '-Yes-'                                |      (2)  |
                                         +-NAS-----+
                                         '-Servidor-'

>+-----+-----+-----+-----+-----+----->
  '-URL---url-'  '-UTILITYUrl---utility_url-'

      .-MAXNUMMP---1----- . -AUTOFSRename---No----- .
>+-----+-----+-----+-----+-----+----->
  '-MAXNUMMP---number-'  '-AUTOFSRename---+Yes---+-'
                                         +-No---+
                                         '-Client-'

      .-KEEPMP---No----- . (3)
>+-----+-----+-----+-----+-----+----->
  '-KEEPMP---+No---+-'
      '-Yes-'

      .-VALIDateprotocol---No----- .
>+-----+-----+-----+-----+-----+----->
  '-VALIDateprotocol---+No---+-'
      +-Dataonly+
      '-All-----'

      .-TXNGroupmax---0----- .
>+-----+-----+-----+-----+-----+----->
  '-TXNGroupmax---+0---+-'
      '-numero-'

      .-DATAWritepath---ANY----- .
>+-----+-----+-----+-----+-----+----->
  '-DATAWritepath---+ANY---+-'
      +-LAN---+
      '-LANFree-'

      .-DATAReadpath---ANY----- .
>+-----+-----+-----+-----+-----+----->
  '-DATAReadpath---+ANY---+-'
      +-LAN---+
      '-LANFree-'

>+-----+-----+-----+-----+-----+----->
  '-TARGETLevel---V.R.M.F-'

      .-SESSIONInitiation---Clientorserver----- .
>+-----+-----+-----+-----+-----+----->
  '-SESSIONInitiation---+Clientorserver-----+-'
      '-SERVEROnly--HLAddress---dirección_ip--LLAddress---puerto_tcp-'

>+-----+-----+-----+-----+-----+----->
  '-HLAddress---dirección_ip--LLAddress---puerto_tcp-'

>+-----+-----+-----+-----+-----+----->
  '-EMAILAddress---ID_usuario@nodo-'

      .-DEDUPlication---Clientorserver----- .
>+-----+-----+-----+-----+-----+----->
  '-DEDUPlication---+Clientorserver---+-'
      '-SERVEROnly-----'

      .-BACKUPInitiation---All----- .
>+-----+-----+-----+-----+-----+----->
  |                                |      (4)  |
  '-BACKUPInitiation---+All---+-'
      '-ROOT-'

>+-----+-----+-----+-----+-----+----->
  '-REPLState---+Enabled---+-'
      '-DISabled-'

      .-BKREPLRuledefault---DEFAULT----- .
>+-----+-----+-----+-----+-----+----->
  | (5) |
  '-----BKREPLRuledefault---+ALL_DATA-----+-'
      +-ACTIVE_DATA-----+
      +-ALL_DATA_HIGH_PRIORITY-----+
      +-ACTIVE_DATA_HIGH_PRIORITY+

```

```

                +-DEFAULT-----+
                |-NONE-----|

.-ARREPLRuledefault-----DEFAULT-----
>-----+-----+-----+-----+----->
|   (5)   |-----ARREPLRuledefault-----+-----+-----|
|   |   |               +-ALL_DATA-----+-----+-----+
|   |   |               +-ALL_DATA_HIGH_PRIORITY-+
|   |   |               +-DEFAULT-----+
|   |   |               |-NONE-----|
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

.-SPREPLRuledefault-----DEFAULT-----
>-----+-----+-----+-----+----->
|   (5)   |-----SPREPLRuledefault-----+-----+-----|
|   |   |               +-ALL_DATA-----+-----+-----+
|   |   |               +-ALL_DATA_HIGH_PRIORITY-+
|   |   |               +-DEFAULT-----+
|   |   |               |-NONE-----|
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

.-RECOVERDamaged-----Yes-----
>-----+-----+-----+-----+----->
|   |   |   +-Yes-+ | |
|   |   |   |-No-- |
|   |   |
|   |   |
|   |   |
|   |   |

.-ROLEOVERRIDE-----Userreported-----
>-----+-----+-----+-----+----->
|   |   |   +-Client-----+ |
|   |   |   +-Server-----+
|   |   |   +-Other-----+
|   |   |   |-Userreported- |
|   |   |
|   |   |
|   |   |

(6)
|-----AUTHentication-----LOCAL-----
>-----+-----+-----+-----+----->
|   |   |   +-LOCAL-+ | |
|   |   |   |-LDap-- |
|   |   |
|   |   |

(7)
.-SSLrequired-----Default-----
>-----+-----+-----+-----+----->
|   |   |   +-Yes-----+ |
|   |   |   +-No-----+
|   |   |   +-Default-----+
|   |   |   |-SERVERonly- |
|   |   |
|   |   |
|   |   |

.-SESSIONSECurity-----TRANSitional-----
>-----+-----+-----+-----+----->
|   |   |   +-STRict-----+ | |
|   |   |   |-TRANSitional- |
|   |   |
|   |   |

.-SPLITLARGEObjects-----Yes-----
>-----+-----+-----+-----+-----><
|   |   |   +-Yes-+ | |
|   |   |   |-No-- |
|   |   |
|   |   |
|   |   |
|   |   |

```

Notas:

1. El mandato PASSEXP no se aplica a los administradores que se autentican con un servidor de directorios Lightweight Directory Access Protocol (LDAP).
2. Este parámetro sólo está disponible para sistemas operativos AIX, Linux, Solaris y Windows.
3. El parámetro VALIDATEPROTOCOL está en desuso.
4. El parámetro BACKUPINITIATION se ignora si el sistema operativo del nodo cliente no está soportado.
5. Sólo puede especificar el parámetro BKREPLRULEDEFAULT, ARREPLRULEDEFAULT o SPREPLRULEDEFAULT si especifica el parámetro REPLSTATE.
6. El valor predeterminado puede cambiar si emitió el mandato SET DEFAULTAUTHENTICATION y especificó LDAP.
7. El parámetro SSLREQUIRED está en desuso.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se ha de registrar. La longitud máxima del nombre es de 64 caracteres.

No se puede especificar NONE como nombre de nodo.

contraseña

Especifica la contraseña del nodo cliente, que tiene una longitud máxima de 64 caracteres.

Si autentica contraseñas localmente con el servidor IBM Spectrum Protect, debe especificar una contraseña. La contraseña no es sensible a las mayúsculas y minúsculas.

Si autentica contraseñas con un servidor LDAP, no especifique ninguna contraseña en el mandato REGISTER NODE.

PASSExp

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña 0 – 9999 días. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, se utiliza el período de caducidad de contraseña común del servidor. El período de caducidad de contraseña común es de 90 días, a menos que se haya cambiado emitiendo el mandato SET PASSEXP.

Puede cambiar el período de caducidad de la contraseña mediante los mandatos UPDATE NODE o SET PASSEXP. Puede emitir el mandato SET PASSEXP para establecer un período de caducidad común para todos los administradores y nodos cliente. También puede utilizar el mandato para establecer períodos de caducidad de contraseña de forma selectiva. Si establece un período de caducidad de la contraseña de forma selectiva mediante el mandato REGISTER NODE, el mandato UPDATE NODE o el mandato SET PASSEXP, el período de caducidad se excluirá de los períodos de caducidad de contraseñas comunes que se han creado mediante el mandato SET PASSEXP.

Puede utilizar el mandato RESET PASSEXP para restablecer el período de caducidad de contraseñas en un período de caducidad común. El mandato PASSEXP no se aplica a los nodos que se autentican con un servidor LDAP.

USerid

Especifica el identificador de usuario de administración con autorización de propietario de cliente. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

NONE

Especifica que no se crea ningún ID de usuario de administración. Este es el valor predeterminado.

id_usuario

Especifica que se crea un ID de usuario de administración con el nombre especificado. Puede utilizar este parámetro para otorgar autorización de propietario de cliente a un identificador de usuario de administración existente.

Si se registra un nodo que tiene el mismo nombre que un administrador, el método de autenticación del administrador y el valor SSLREQUIRED cambian para que coincidan con el método de autenticación del nodo. Las contraseñas que se comparten entre nodos y administradores con el mismo nombre se mantienen sincronizadas durante un cambio de autenticación.

Si tiene previsto utilizar la opción sin LAN con este nodo, utilice el parámetro USERID para registrar un ID administrativo que coincida con el nombre de nodo.

Para usuarios de servidores LDAP: Si tiene previsto autenticar el nodo con un servidor LDAP, conserve el valor predeterminado (USERID=NONE) o especifique un ID de usuario de administración distinto del nombre de nodo. Si el ID de usuario de administración coincide con el nombre de nodo, es posible que observe un comportamiento inesperado debido a cambios automáticos de contraseña que actualizan la misma contraseña dos veces. Como resultado, la contraseña podría llegar a ser desconocida para el ID de usuario de administración. De forma alternativa, la operación de actualización de contraseña podría fallar.

CONtact

Especifica una serie de texto de información que identifica el nodo. El parámetro es opcional. La longitud máxima de la serie de texto es de 255 caracteres. La información de contacto debe estar encerrada entre comillas, si contiene espacios en blanco.

DOmain

Especifica el nombre del dominio de políticas al que se asigna el nodo. El parámetro es opcional. Si no especifica un nombre de dominio de políticas, se asigna el nodo al dominio de políticas predeterminado (STANDARD).

Si un servidor origen está inscrito como un nodo, se asigna a un dominio de políticas. Los datos del servidor de origen se almacenan en la agrupación de almacenamiento especificada en el grupo de copia archivada de la clase de gestión predeterminada de dicho dominio.

COMPrission

Especifica si el nodo cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado. El parámetro es opcional. El valor predeterminado es CLIENT.

Restricción: Este parámetro no se aplica a los nodos con un tipo NAS o SERVER.

Puede especificar uno de los siguientes valores:

Client

Especifica que el cliente determina si se han de comprimir los archivos.

Yes

- No Especifica que el nodo cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado.
- No Especifica que el nodo cliente no comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado.

ARCHDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. El parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

- Yes Especifica que el nodo cliente puede suprimir sus propias copias archivadas del servidor.
- No Especifica que el nodo cliente no puede suprimir sus propias copias archivadas del servidor.

BACKDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

- No Especifica que el nodo cliente no puede suprimir sus propias copias de seguridad del servidor.
- Yes Especifica que el nodo cliente puede suprimir sus propias copias de seguridad del servidor.

CLOptset

Especifica el nombre del conjunto de opciones que ha de utilizar el cliente. El parámetro es opcional.

FORCEPwreset

Especifica si se forzará que un cliente cambie o restablezca la contraseña. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

- No Especifica que el período de caducidad de contraseña se establece mediante el mandato SET PASSEXP. El cliente no necesita cambiar ni restablecer la contraseña cuando el cliente está iniciando la sesión en el servidor.
- Yes Especifica que la contraseña del nodo cliente caducará en la próxima conexión. El cliente debe cambiar o restablecer la contraseña. Si no se especifica una contraseña, recibirá un mensaje de error.
Restricción: En el caso de los nodos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizan los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si especifica AUTHENTICATION=LDAP.

Type

Especifica el tipo de nodo que se está inscribiendo. El parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

- Client Especifica que el nodo de cliente es un cliente de archivado y copia de seguridad, un cliente de IBM Spectrum Protect for Space Management o un cliente de aplicaciones.
- NAS Especifica que el nodo es un servidor de archivos de almacenamiento conectado a red (NAS) cuyos datos se protegen mediante operaciones NDMP. El nombre de nodo no puede ser SERVER.
Nota: El nombre del nodo NAS debe ser el mismo que el del transportador de datos. Por lo tanto, el nombre no puede cambiarse después de haberse definido el transportador de datos correspondiente.
- Server Especifica que el nodo de cliente es un servidor de origen que se está inscribiendo en el servidor de destino.

URL

Especifica el URL del cliente web de IBM Spectrum Protect que se ha configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

Este parámetro es opcional. El URL debe incluir el nombre DNS o la dirección IP del sistema cliente y el número de puerto que está definido en el sistema cliente para el cliente web de IBM Spectrum Protect. Por ejemplo,
`http://client.mycorp.com:1581`

UTILITYUrl

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde Centro de operaciones.

Este parámetro es opcional. Puede especificar un URL de hasta 200 caracteres de longitud. El URL debe empezar por `https`. Incluye el nombre DNS o la dirección IP del sistema cliente y el número de puerto que se ha definido en el sistema cliente para los servicios de gestión de cliente de IBM Spectrum Protect. Por ejemplo, `https://client.mycorp.com:9028`

Si se omite el número de puerto, el Centro de operaciones utiliza el número de puerto 9028, que es el número de puerto predeterminado cuando se instalan los servicios de gestión del cliente en el sistema cliente.

MAXNUMMP

Especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor o en el agente de almacenamiento sólo para las operaciones de copia de seguridad, de archivado y de migración IBM Spectrum Protect for Space Management. El parámetro es opcional y no se aplica a los nodos con un tipo NAS o SERVER. El valor predeterminado es 1. Puede especificar un entero en el rango de 0 a 999. Un valor de 0 especifica que un nodo no puede adquirir ningún punto de montaje para una operación de almacenamiento de datos de cliente. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos las operaciones de almacenamiento de datos simultáneas del mismo nodo cliente, y puede que impidan que las operaciones de almacenamiento de datos obtengan puntos de montaje.

En el caso de los volúmenes de una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA, el servidor puede disponer, simultáneamente, de varias sesiones que lean y de un único proceso que grabe en el mismo volumen. Para aumentar la concurrencia y proporcionar un acceso eficiente para nodos que tienen datos en agrupaciones de almacenamiento FILE o CENTERA, incremente el valor del parámetro MAXNUMMP.

En nodos que almacenan datos en agrupaciones de almacenamiento primarias con la función de grabación simultánea activada, deberá ajustar el valor del parámetro MAXNUMMP para especificar el número correcto de puntos de montaje de cada sesión de cliente. Una sesión de cliente requiere un punto de montaje para la agrupación de almacenamiento primario y un punto de montaje para cada agrupación de almacenamiento de copias y cada agrupación de datos activos.

Para una copia de seguridad de servidor a servidor, si un servidor se encuentra en una versión diferente de la de otro servidor, establezca el número de puntos de montaje en el servidor de destino en un valor superior a uno. De lo contrario, recibirá un error.

Un agente de almacenamiento hace un seguimiento del número de puntos empleados durante una sesión de cliente de forma independiente. Si un nodo tiene un agente de almacenamiento que se ha instalado, puede superar el valor de MAXNUMMP. El valor MAXNUMMP puede superarse también en condiciones en que el nodo no tiene que esperar un punto de montaje.

Nota: El servidor puede tomar el control de la operación de un cliente para una operación de prioridad superior y el cliente puede perder un punto de montaje si no hay ningún otro punto de montaje disponible.

KEEPMP

Especifica si el nodo cliente mantiene el punto de montaje durante toda la sesión. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

Yes

Especifica que el nodo cliente debe retener el punto de montaje durante toda la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se retendrán los puntos de montaje que mantenga la sesión.

No

Especifica que el nodo de cliente libera el punto de montaje durante la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se publicarán los puntos de montaje que mantenga la sesión.

AUTOFSRename

Especifique si el nombre de los espacios de archivos ha de cambiarse automáticamente al actualizar el sistema cliente para el soporte de Unicode o especifique si el cliente ha de realizar, si es necesario, el cambio del nombre de los espacios de archivos. El parámetro es opcional. El valor predeterminado es NO. El establecimiento del parámetro en YES activa el cambio automático del nombre, que tiene lugar cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. El cambio automático del nombre cambia los nombres de los espacios de archivos existentes de los que se ha realizado una copia de seguridad y que no están en Unicode en el almacenamiento del servidor. A continuación, se realiza una copia de seguridad de los espacios de archivos en Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS X y NetWare.

Una vez que se ha instalado el cliente que admite Unicode, los nuevos espacios de archivos de los que el cliente hace una copia de seguridad se almacenan en el almacenamiento del servidor utilizando la página de códigos UTF-8. UTF-8 es un formato de codificación orientado a bytes que especifica el estándar de Unicode.

Puede especificar uno de los siguientes valores:

Yes

El nombre de los espacios de archivos existentes se cambia automáticamente al actualizar a un cliente que admite Unicode y cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental o copia de seguridad parcial incremental. La redenominación se produce si el cliente utiliza una interfaz gráfica de usuario, la línea de mandatos o el planificador cliente.

Por ejemplo, el servidor redenomina una unidad del siguiente modo:

```
Nombre original: D_DRIVE  
Nombre nuevo: D_DRIVE_OLD
```

El nombre nuevo indica que el espacio de archivos se almacena en el servidor en un formato que no es Unicode.

No

Los espacios de archivos no se redenominan automáticamente cuando el sistema cliente se actualiza a un cliente que admite Unicode y el cliente ejecuta una de las siguientes operaciones: archivado, copia de seguridad selectiva, copia de seguridad incremental o copia de seguridad parcial incremental.

Client

La opción AUTOFSDRENAME en el archivo de opciones del cliente determina si los espacios de archivos están redenominados.

De forma predeterminada, la opción de cliente se define en PROMPT. Cuando el sistema cliente se actualiza en un cliente compatible con Unicode y el cliente realiza una operación de IBM Spectrum Protect con la interfaz gráfica de usuario o la línea de mandatos, el programa pregunta una vez al usuario si desea cambiar el nombre los espacios de archivos.

Cuando el planificador cliente realiza una operación, el programa no ofrece ninguna solicitud sobre redenominación y no redenomina los espacios de archivos. Las copias de seguridad de los espacios de archivos existentes se envían como antes (no en Unicode).

VALIDateprotocol (en desuso)

Especifica si IBM Spectrum Protect completa una comprobación de redundancia cíclica para validar los datos que se han enviado entre el cliente y el servidor. El parámetro es opcional. El valor predeterminado es NO.

Importante: A partir de IBM Spectrum Protect V8.1.2 y Tivoli Storage Manager Versión 7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

TXNGroupmax

Especifica el número de archivos por validación de transacción que se transfieren entre un cliente y un servidor. El parámetro es opcional. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.

El valor predeterminado es 0. Al especificar 0 se indica que el nodo utiliza el valor global del servidor que se ha establecido en el archivo de opciones del servidor. Si desea emplear un valor distinto del valor global del servidor, especifique un valor entre 4 y 65.000 para este parámetro. El valor del nodo prevalece sobre el valor del servidor.

Atención: Si aumenta el valor de TXNGROUPMAX, aumenta la utilización del registro de recuperación. Una mayor utilización del registro de recuperación puede incrementar el riesgo de quedarse sin espacio de registro. Evalúe el rendimiento de cada uno de los nodos antes de cambiar este parámetro.

DATAWritepath

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento tales como copia de seguridad o archivado. El parámetro es opcional. El valor predeterminado es ANY.

Nota: Si no hay disponible una ruta, el nodo no puede enviar ningún dato. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará.

Puede especificar uno de los siguientes valores:

ANY

Especifica que los datos se envían al servidor, agente de almacenamiento o a ambos por medio de cualquier ruta disponible. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se mueven mediante la LAN.

LAN

Especifica que los datos se envían utilizando la LAN.

LANFree

Especifica que los datos se envían utilizando una ruta fuera de la LAN.

DATAReadpath

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. El parámetro es opcional. El valor predeterminado es ANY.

Nota: Si no hay disponible una ruta, no es posible leer datos. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará. El valor de la vía de acceso de transferencia también se aplica a las conexiones de migración tras error. Si el valor se establece en LANFree, puede producirse la migración tras error para el nodo en el servidor secundario.

Puede especificar uno de los siguientes valores:

ANY

Especifica que el servidor, agente de almacenamiento o ambos utilizan cualquier ruta disponible para leer datos. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se leen utilizando la LAN.

LAN

Especifica que los datos se leen utilizando la LAN.

LANFree

Especifica que los datos se leen utilizando una ruta fuera de la LAN.

TARGETLevel

Especifica el paquete de despliegue del cliente que se utiliza este nodo. Puede sustituir con un paquete de release aplicable Version.Release.Modification.Fix (V.R.M.F) Level. Por ejemplo: TARGETLevel=6.2.0.0.

Debe especificar cada segmento con un número aplicable a un paquete de despliegue. No se puede utilizar el asterisco en ningún campo como sustituto de un número válido. El parámetro es opcional.

Restricción: El parámetro TARGETLEVEL no se aplica a los nodos con un tipo NAS o SERVER.

SESSIONINITiation

Controla si el servidor o el cliente ha de iniciar las sesiones. El valor predeterminado establece que el cliente ha de iniciar las sesiones. El parámetro es opcional.

Clientorserver

Especifica que el cliente puede iniciar sesiones con el servidor comunicándose en el puerto TCP/IP que se ha definido con la opción de servidor TCPPORT. También puede utilizarse la planificación por petición de servidor para solicitar al cliente que se conecte con el servidor.

SERVEROnly

Especifica que el servidor no acepta peticiones de sesiones del cliente. Todas las sesiones deberá iniciarlas la planificación por petición de servidor en el puerto que se ha definido para el cliente con los mandatos REGISTER o UPDATE NODE. No se puede utilizar Client Acceptor, dsmscad, para iniciar el planificador si SESSIONINITIATION está establecido en SERVERONLY.

HLAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

EMAILAddress

Este parámetro se utiliza para obtener más información de contacto. El parámetro es opcional. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

DEDUPlication

Especifica dónde puede producirse la eliminación de datos duplicados para este nodo. El parámetro es opcional. Puede especificar uno de los siguientes valores:

Clientorserver

Indica que los datos almacenados por este nodo se pueden deduplicar en el cliente o en el servidor. Este es el valor predeterminado. Para realizar la eliminación de datos duplicados en el cliente, debe especificar el valor YES en la opción de cliente DEDUPLICATION. Puede especificar esta opción en el archivo de opciones del cliente o en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

SERVEROnly

Especifica que los datos almacenados por este nodo sólo se pueden deduplicar en el servidor.

BACKUPINITiation

Especifica si el ID de usuario no root en el nodo de cliente puede realizar una copia de seguridad de los archivos en el servidor. El parámetro es opcional. El valor predeterminado es ALL, que indica que los ID de usuario no root pueden realizar una copia de seguridad de los datos en el servidor. Puede seleccionar uno de los siguientes valores:

All

Especifica que los ID de usuario no root pueden realizar una copia de seguridad de los archivos en el servidor. ALL es el valor predeterminado si no se especifica BACKUPINITIATION.

ROOT

Especifica que el ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor. Si utiliza el cliente de copia de seguridad-archivador V6.4 o posterior, los usuarios autorizados tiene los mismos privilegios que el ID de usuario root.

Restricción: El servidor ignora el atributo si el cliente de archivado y copia de seguridad se conecta desde un sistema operativo distinto de AIX, Linux, Solaris o Mac OS.

Recuerde: La interfaz de programación de aplicaciones (API) se ve afectada por el parámetro BACKUPINITIATION en el servidor. De forma predeterminada, a todos los usuarios de la API se les permite realizar una copia de seguridad de los datos. No se recomienda establecer el parámetro en ROOT en un nodo de la API.

REPLState

Especifica si los datos que pertenecen al nodo de cliente están preparados para replicarse. Este parámetro es opcional.

Especifica este parámetro sólo si emite el mandato REGISTER NODE en un servidor que está configurado para replicar datos en un servidor de réplica de destino. Si registra un nodo de cliente en un servidor de réplica de origen y configura la réplica para el nodo, no registre el nodo en el servidor de réplica de destino. El nodo de cliente se crea automáticamente en el servidor de destino la primera vez que se produce la réplica.

Puede seleccionar uno de los siguientes valores:

ENabled

Especifica que el nodo de cliente está configurado para la réplica y preparado para replicarse. Cuando especifica este parámetro, la modalidad de réplica en la definición de nodo de cliente en el servidor de réplica de origen se establece automáticamente en SEND. Este valor indica que los datos que pertenecen al nodo de cliente se envían a un servidor de destino durante la réplica.

Cuando se realiza la réplica por primera vez para el nodo de cliente, el estado de réplica del nodo en el servidor de réplica de destino se establece automáticamente en ENABLED. La modalidad de réplica en el servidor de réplica de destino se establece en RECEIVE. Este valor indica que los datos que pertenecen al nodo de cliente se reciben de un servidor de réplica de origen. Para determinar la modalidad y el estado de la réplica, emita el mandato QUERY NODE en un servidor de réplica de origen o destino.

DISabled

Especifica que el nodo está configurado para la réplica, pero que la réplica no se produce hasta que la activa.

BKREPLRuledefault, ARREPLRuledefault, y SPREPLRuledefault

Especifica la regla de réplica que se aplica a un tipo de datos si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT.

Restricción: Sólo puede especificar el parámetro BKREPLRULEDEFAULT, ARREPLRULEDEFAULT o SPREPLRULEDEFAULT si especifica el parámetro REPLSTATE.

BKREPLRuledefault

Especifica la regla de réplica de los datos de copia de seguridad.

ARREPLRuledefault

Especifica la regla de réplica de los datos de archivado.

SPREPLRuledefault

Especifica la regla de réplica de los datos gestionados por espacio.

Si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT y no especifica una regla para el parámetro BKREPLRULEDEFAULT, ARREPLRULEDEFAULT o SPREPLRULEDEFAULT, los datos se replican según la regla de servidor del tipo de datos.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Puede especificar las siguientes reglas:

ALL_DATA

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal. Esta regla sólo es válida para BKREPLRULEDEFAULT.

Atención:

Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando se instala una versión anterior a la Versión 7.1.1 en los servidores de réplica de origen o de destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la duplicación, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino de una versión anterior a V7.1.1.

Si las condiciones anteriores no son verdaderas, se duplican todos los archivos nuevos y cambiados desde la última réplica, incluidos los archivos inactivos, y los archivos se suprimen cuando caducan.

ALL_DATA_HIGH_PRIORITY

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE_DATA excepto que los datos se replican con una prioridad alta. Esta regla sólo es válida para BKREPLRULEDEFAULT.

DEFAULT

Replica los datos según la regla de réplica del servidor para los datos de copia de seguridad.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es especificar `ARREPLRULEDEFAULT=DEFAULT`. Asegúrese de que las reglas de espacio de archivos de los datos de archivado también se establezcan en DEFAULT y que la regla del servidor de los datos de archivado se establezca en ALL_DATA_HIGH_PRIORITY.

Restricción: Si se configura un nodo para la réplica, las reglas de espacio de archivos se establecen en DEFAULT después de que el nodo almacene datos en el servidor de réplica de origen.

NONE

Los datos del tipo especificado no se replican.

Por ejemplo, si no desea replicar los datos gestionados por espacio que pertenecen a un nodo de cliente, especifique `SREPLRULEDEFAULT=NONE`

RECOVERDamaged

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino. El parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino está habilitada para este nodo.

No

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino no está habilitada para este nodo.

Consejo: El valor del parámetro RECOVERDAMAGED es sólo uno de varios valores que determinan si se recuperan los archivos dañados. Para obtener información sobre cómo especificar los valores, consulte Valores que afectan a la recuperación de archivos dañados.

ROLEOVERRIDE

Especifica si se debe alterar temporalmente el rol notificado del cliente para la creación de informes de estimación de unidades de valor de procesador (PVU). El valor predeterminado es USEREPORTED. El parámetro es opcional.

El rol notificado por el cliente es un dispositivo de cliente (por ejemplo, una estación de trabajo) o un dispositivo de servidor (por ejemplo, un servidor de archivos/impresión, un servidor de aplicaciones o una base de datos). De forma predeterminada, el cliente notifica su rol basándose en el tipo de cliente y el sistema operativo. Todos los clientes notifican inicialmente su rol como dispositivo de servidor, excepto los clientes de archivado y copia de seguridad que ejecutan distribuciones de estaciones de trabajo de Microsoft Windows (Windows Vista) y Macintosh OS X.

Especifique uno de los siguientes valores:

Client

Especifica un dispositivo de cliente.

Server

Especifica un dispositivo de servidor.

Otro

Especifica que este nodo no se va a utilizar para la creación de informes de estimaciones de PVU. Este valor puede ser útil cuando se despliegan múltiples nodos para un sistema físico (por ejemplo, entornos virtuales, nodos de prueba, nodos retirados y nodos que no estén en producción ni en clúster).

Usereported

Utilice el rol notificado que proporciona el cliente.

AUTHentication

Este parámetro especifica el método de autenticación de contraseña para el nodo. Especifique uno de los siguientes valores: LDAP o LOCAL. El parámetro es opcional y toma el valor predeterminado LOCAL. El valor predeterminado se puede cambiar a LDAP si se utiliza el mandato SET DEFAULTAUTHENTICATION y especifica LDAP.

Local

Especifica que se está utilizando la base de datos del servidor IBM Spectrum Protect .

LDap

Especifica que el nodo utiliza un servidor LDAP para la autenticación de contraseñas.

SSLrequired (en desuso)

Especifica si el nodo debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect . El parámetro es opcional. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red

Importante: A partir del software de IBM Spectrum Protect V8.1.2 y del software de Tivoli Storage Manager V7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

SESSIONSECurity

Especifica si el nodo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el nodo. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el nodo pueda autenticarse en el servidor:

- Tanto el nodo como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el nodo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el nodo.

Los nodos que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

TRANSitional

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el nodo no cumplen nunca los requisitos para el valor STRICT, el nodo continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un nodo cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el nodo ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con

los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, el nodo ya no se puede autenticar con un protocolo menos seguro. Por ejemplo, si se actualiza un nodo que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, cuando el nodo se autentica en el servidor IBM Spectrum Protect como nodo de otro servidor.

SPLITLARGEObjects

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. El parámetro es opcional. Si se especifica Sí, el servidor divide los objetos grandes (más de 10 GB) en partes más pequeñas cuando se almacenan en un nodo de cliente. Si se especifica No, se ignora este proceso. Especifique No solo si lo que pretende es maximizar el rendimiento de las copias de seguridad directamente en la cinta. El valor predeterminado es Yes (sí).

Ejemplo: registrar un nodo de cliente del que sólo puede hacer una copia de seguridad el usuario root

Registre el nodo de cliente `mete0rite` con la contraseña `KingK0ng` para permitir que sólo el usuario `root` pueda realizar una copia de seguridad de los archivos en el servidor.

```
register node mete0rite KingK0ng
backupinit=root
```

Ejemplo: registrar un nodo cliente y una contraseña y activar la compresión

Registrar el nodo cliente `JOEOS2` con la contraseña `SECRETCODE` y asignar este nodo al dominio de políticas `DOM1`. Este nodo puede suprimir sus propias copias de seguridad y copias archivadas del servidor. Todos los archivos los comprime el nodo cliente antes de enviarlos al servidor. Este mandato creará automáticamente el identificador de usuario de administración `JOEOS2` con la contraseña `SECRETCODE`. Asimismo, el administrador ahora dispondrá de autorización de propietario de cliente para el nodo `JOEOS2`.

```
register node joeos2 secretcode domain=dom1
archdelete=yes backdelete=yes
compression=yes
```

Ejemplo: otorgar autorización de propietario de cliente a un usuario de administración existente

Otorgar autorización de propietario de cliente a un ID de usuario de administración existente, `HELPAADMIN`, al registrar el nodo cliente `JAN`. Este paso no creará automáticamente un ID de administrador denominado `JAN`, sino que otorgará autorización de propietario de cliente para este nodo al administrador `HELPAADMIN`.

```
register node jan pwdsafe userid=helpadmin
```

Ejemplo: registrar un nodo servidor de archivos que utiliza operaciones NDMP

Registrar el nombre de nodo `NAS1` para un servidor de archivos NAS que utiliza operaciones NDMP. Asignar este nodo a un dominio NAS especial.

```
register node nas1 pw4pw domain=nasdom type=nas
```

Ejemplo: registrar un nodo y especificar el número máximo de archivos por validación de transacción

Registrar el nombre de nodo `ED` y establecer el valor `TXNGroupmax` en 1.000.

```
register node ed pw45twx txngroupmax=1000
```

Ejemplo: registrar un nodo y permitirle eliminar duplicados en el sistema cliente

Registre el nombre de nodo `JIM` y permítale eliminar duplicados de datos en el sistema cliente.

```
register node jim jim deduplication=clientorserver
```

Ejemplo: registrar un nombre de nodo ED y establecer el rol como un dispositivo de servidor para la creación de informes de estimación de PVU

Registre un nombre de nodo `ED` y establezca el rol como un dispositivo de servidor para la creación de informes de estimación de PVU.

```
register node ed pw45twx roleoverride=server
```

Ejemplo: registrar un nodo en un servidor de réplica de origen

Defina NODE1 en un servidor de réplica de origen. Especifique una regla de réplica para los datos de copia de seguridad que pertenecen a NODE1, para que los datos de copia de seguridad activos se repliquen con una prioridad alta. Active la réplica para el nodo.

```
register node node1 bkreplruledefault=active_data_high_priority replstate=enabled
```

Ejemplo: registrar un nodo que se autentique mediante un servidor LDAP

Registre un nombre de nodo de NODE17 que debe autenticarse con un servidor LDAP.

```
register node node17 authentication=ldap
```

Consejo: Al registrar un nodo de esta forma, no se crea un ID de usuario de administración.

Ejemplo: Registrar un nodo para comunicarse con un servidor utilizando la seguridad de sesión transitoria.

Registre un nombre de nodo, NODE4, para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
register node node4 sessionsecurity=strict
```

Ejemplo: Registrar un nodo y habilitar la recuperación de archivos dañados

Registrar un nombre de nodo PAYROLL. Para el nodo PAYROLL, habilite la recuperación de archivos dañados a partir de un servidor de réplica de destino.

```
register node payroll recoverdamaged=yes
```

Mandatos relacionados

Tabla 2. Mandatos relacionados con REGISTER NODE

Mandato	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.

Mandato	Descripción
RENAME NODE	Cambia el nombre de un nodo cliente.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

Conceptos relacionados:




[🔗](#) Cliente raíz de UNIX y Linux y tareas de usuario autorizadas

Referencia relacionada:

[🔗](#) Opción de cliente SSL

Mandatos REMOVE

Utilice los mandatos REMOVE para eliminar un objeto de IBM Spectrum Protect.

- REMOVE ADMIN (Suprimir un ID de usuario administrador)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)
- REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)
- REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)
- REMOVE REPLSERVER (Eliminar un servidor de réplica)

REMOVE ADMIN (Suprimir un ID de usuario administrador)

Utilice este mandato para suprimir un ID de usuario administrador del sistema.

No puede eliminar el ID de usuario administrador del sistema o el ID administrativo SERVER_CONSOLE del sistema.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-SYNClapdelete-----No----->
>>-REMove Admin--nombre_admin-----+-----><
      '-SYNClapdelete-----+No--+-'
      '-Yes-'

```

Parámetros

nombre_admin (Necesario)

Especifica el ID de usuario administrador que se ha de eliminar.

SYNClapdelete

Especifica si desea suprimir el ID de usuario de administración en el servidor LDAP (Lightweight Directory Access Protocol).

Sí

Suprime el ID de usuario de administración en el servidor LDAP.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

No suprime el ID de usuario de administración en el servidor LDAP. Este es el valor predeterminado.

Ejemplo: Suprimir un ID de usuario administrador




Suprime el ID de usuario administrador larry que no está definido en un servidor LDAP. Emita el mandato siguiente:

```
remove admin larry
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REMOVE ADMIN

Mandato	Descripción
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)

Tras la conversión de la agrupación de almacenamiento, utilice este mandato para eliminar los datos dañados de una agrupación de almacenamiento que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL).

El mandato REMOVE DAMAGED suprime de forma permanente los datos dañados de la agrupación de almacenamiento.

Consejo: antes de eliminar los datos dañados de la agrupación de almacenamiento, intente recuperar una versión sin daños de los datos de una agrupación de almacenamiento de copia o de datos activos emitiendo el mandato RESTORE STGPOOL. Recupere una versión sin daños de los datos de un servidor de réplica de destino emitiendo el mandato REPLICATE NODE y especificando el parámetro RECOVERDAMAGED=YES.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

Sintaxis

```

      .-*----->
>>-REMove DAMaged--nombre_agrupación-----+----->
      | .-|----->
      | V |----->

```



```

                      '---nombre_nodo---'
.-Wait-----No-----
>-----<
'-Wait-----No---'
                   '-Yes-'

```

Parámetros

nombre_agrupación (Obligatorio)

Especifique una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL). La agrupación de almacenamiento contiene los datos dañados. Este parámetro es obligatorio.

nombre_nodo

Especifica el nombre del nodo cliente. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar un carácter comodín en lugar de un nombre de nodo si desea eliminar daños de todos los nodos de la agrupación de almacenamiento.

Wait

Especifica si se debe esperar al servidor para eliminar datos dañados de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar este parámetro solamente desde una línea de mandatos administrativa. Puede especificar uno de los siguientes valores:

No

Especifica que el mandato se procesa de forma subordinada.

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

Ejemplo: eliminar datos dañados de una agrupación de almacenamiento y esperar a que el servidor complete el proceso

Eliminar los datos dañados de una agrupación de almacenamiento llamada POOL1 y esperar a que el servidor complete el proceso en primer plano.

```
remove damaged pool1 wait=yes
```

Tabla 1. Mandatos relacionados con REMOVE DAMAGED

Mandato	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.

REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)

Utilice este mandato para suprimir un nodo del servidor. Si está utilizando el gestor de recuperación ante siniestro y el nodo que se ha de suprimir está asociado a una máquina, se suprimirá también la asociación entre el nodo y la máquina.

Si el nodo es miembro de un grupo de proximidad y elimina el nodo del servidor, el nodo también se elimina del grupo de proximidad. Si se elimina un nodo y este contenía espacios de archivos en un grupo de proximidad de espacio de archivos, estos espacios de archivos se eliminan de la lista de miembros del grupo.

Si elimina un nodo que almacenó datos en una agrupación de almacenamiento de duplicados eliminados, el nombre del nodo DELETED se visualiza en la salida del mandato QUERY OCCUPANCY hasta que todas las dependencias de eliminación de duplicados de datos se eliminan.

Cuando se elimina un nodo, el ID de administración correspondiente se elimina solamente si se cumplen las condiciones siguientes:

- El nombre del administrador es idéntico al nombre del nodo.
- El administrador tiene autorización de propietario de cliente o de acceso a cliente *solo* para el nodo que se elimina.
- El administrador no es un objeto gestionado.

Para poder suprimir un nodo, debe suprimir todos los espacios de copia de seguridad y copia archivada que pertenezcan a dicho nodo. Antes de poder eliminar un nodo NAS que tenga un transportador de datos correspondiente, debe completar las tareas siguientes en orden:

1. Suprimir las rutas desde el transportador de datos
2. Suprimir el transportador de datos
3. Suprimir todas las definiciones de espacio de archivos virtual para el nodo
4. Eliminar el nodo NAS

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```

>>-REMOve Node--nombre_nodo--+-SYNCLdapdelete-----No-----+----->>
                               '-SYNCLdapdelete-----+No--+-'
                               '-Yes-'

```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo que se ha de suprimir.

SYNCLdapdelete

Especifica si debe eliminarse el nodo del servidor LDAP (Lightweight Directory Access Protocol).

Sí

Especifica que el nodo se elimina.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que el nodo no se elimina. Este es el valor predeterminado.





Ejemplo: eliminar un nodo cliente



Eliminar el nodo cliente LARRY.

```
remove node larry
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REMOVE NODE

Mandato	Descripción
 Sistemas operativos AIX  Sistemas operativos Windows DELETE MACHNODEASSOCIATION	 Sistemas operativos AIX  Sistemas operativos Windows Suprime la asociación entre una máquina y un nodo.
DELETE DATAMOVER	Suprimir un transportador de datos.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE PATH	Suprime una ruta de un origen a un destino.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.

Mandato	Descripción
 QUERY MACHINE	 Muestra información sobre máquinas.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RENAME NODE	Cambia el nombre de un nodo cliente.

REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)

Utilice este mandato para eliminar un nodo de la réplica si ya no desea replicar los datos que pertenecen al nodo.

No puede suprimirse los datos del nodo cliente emitiendo el mandato REMOVE REPLNODE. Puede emitir el mandato en un servidor de réplica de origen o de destino. Sólo se puede emitir este mandato desde el cliente de línea de mandatos administrativos. Este mandato no se puede emitir en la consola del servidor.

Si emite el mandato REMOVE REPLNODE para un nodo de cliente cuyo nodo de réplica está establecido en SEND o RECEIVE, la modalidad se establece en NONE. El estado de réplica también se establece en NONE. Después de eliminar un nodo de cliente de la réplica, el servidor de réplica de destino puede aceptar los datos de copia de seguridad, archivado y gestionados por espacio directamente desde el nodo.

Si un nodo de cliente se elimina de la réplica, se suprime la información en la base de datos sobre la réplica del nodo. Si el nodo de cliente se activa para la réplica más adelante, el proceso de réplica replica todos los datos especificados por los valores y las reglas de réplica.

Al emitir el mandato REMOVE REPLNODE, los datos que pertenecen a un nodo de cliente no se suprimen. Para suprimir los datos del espacio de archivos que pertenecen al nodo de cliente, emita el mandato DELETE FILESPACE para cada uno de los espacios de archivos que pertenecen al nodo. Si no desea mantener la definición de nodo de cliente, emita el mandato REMOVE NODE. Para suprimir los datos del espacio de archivos y la definición de nodo de cliente, emita DELETE FILESPACE y REMOVE NODE en el servidor de réplica de destino.

Restricción: Si se está ejecutando un proceso de réplica de nodo para un nodo de cliente especificado por este mandato, el mandato falla y la información de réplica del nodo no se elimina.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```

      .- ,-----
      v |
>>>-REMOve REPLNode-----+-nombre_nodo-----+----->>>
      '-nombre_grupo_nodos-'

```

Parámetros

nombre_nodo o nombre_grupo_nodos (Necesario)

Especifica el nombre del nodo de cliente y del grupo definido de nodos de cliente que desea eliminar de la réplica. Para especificar varios nombres de nodos de cliente y nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede utilizar caracteres comodín para especificar los nombres de nodos de cliente, pero no para especificar los nombres de grupos de nodos de cliente. No puede combinar nombres de nodo o grupo de nodos con el nombre de dominio.

Ejemplo: eliminar tres nodos de cliente y un grupo de nodos de cliente de la réplica

Los nombres de los nodos cliente son NODE1, NODE2 y NODE3. El nombre del grupo de nodos de cliente es PAYROLL. Emita el siguiente mandato en los servidores de réplica de origen y destino:

```
remove replnode node*, payroll
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REMOVE REPLNODE

Mandato	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.

REMOVE REPLSERVER (Eliminar un servidor de réplica)

Utilice este mandato para eliminar o cambiar un servidor de réplica de la lista de servidores de réplica. Este mandato suprime toda la información que existe sobre el estado de la réplica de todos los nodos que se ha copiado en el servidor.

Puede emitir el mandato en un servidor de réplica de origen o de destino.

Restricción: No puede suprimirse los datos del nodo cliente emitiendo el mandato REMOVE REPLSERVER.

Utilice el mandato para conmutar servidores de réplica y eliminar información de réplica de un servidor anterior. El mandato no afecta a la modalidad de réplica ni al estado actual de todas las definiciones de nodo. Emita el mandato en los servidores de origen y de destino para mantener la coherencia de la información de estado de réplica sobre ambos servidores.

Restricción: Si especifica el servidor de réplica predeterminado en el mandato REMOVE REPLSERVER y un proceso de réplica de nodo está en ejecución, el mandato falla y no se elimina ninguna información de réplica.

Este mandato se ejecuta como una operación en segundo plano y no se puede cancelar. IBM Spectrum Protect suprime información de duplicación que está asociada al servidor especificado, como por ejemplo, una serie de transacciones de base de datos por lotes. Si se produce un problema en el sistema, puede realizarse una supresión parcial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REMOve REPLServer--GUID-----<<
```

Parámetros

guid_ réplica (Obligatorio)

Identificador único del servidor de réplica que va a eliminarse. Puede utilizar caracteres comodín para especificar el Identifier exclusivo global de réplica (GUID); sin embargo, solamente puede coincidir un GUID con el comodín. Si la secuencia comodín coincide con más de un GUID, el mandato falla. Debe calificar la serie comodín solamente hasta que se encuentre el GUID que desea suprimir.

Ejemplo: utilizar un comodín para eliminar un servidor de réplica

Elimine un servidor de réplica utilizando un carácter comodín para indicar el GUID de la réplica.

```
remove replserver e*
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REMOVE REPLSERVER

Mandato	Descripción
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	Elimina un nodo de la réplica.

Mandato	Descripción
QUERY REPLSERVER (Consultar un servidor de réplica)	Muestra información sobre servidores de réplica.

Mandatos RENAME

Utilice los mandatos RENAME para cambiar el nombre de un objeto existente.

- RENAME ADMIN (redenominar un administrador)
- RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)
- RENAME NODE (Cambiar el nombre de un nodo)
- RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)
- RENAME SERVERGROUP (Redenominar un grupo de servidores)
- RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)

RENAME ADMIN (redenominar un administrador)

Utilice este mandato para cambiar un ID de usuario administrador. No se modificará la información existente para este administrador, como por ejemplo la información de contacto y las clases de privilegios.

Si asigna un ID de usuario de administración existente a otra persona, utilice el mandato UPDATE ADMIN para cambiar la contraseña.

Cuando un administrador y un nodo comparten nombres y cambia el método de autenticación de administrador, el método de autenticación de nodo también cambia. Si cambia el nombre de un administrador por el mismo nombre que un nodo existente, el método de autenticación y el valor SSLREQUIRED del nodo pueden cambiar. Si estos valores son diferentes, después del cambio de nombre, tanto el administrador y el nodo tendrá el mismo método de autenticación y el mismo valor SSLREQUIRED.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Al cambiar el nombre de un ID de usuario de administración, tenga cuidado de que no coincida con un nombre de nodo. Si los nombres coinciden, es posible que se dé un comportamiento imprevisto, debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría pasar que la actualización de la contraseña fallase.

No puede redenominar el ID de administración SERVER_CONSOLE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REName Admin--nombre_admin_actual--nombre_admin_nuevo----->
      .-SYNClapdelete---No-----
>--+-----+-----><
      '-SYNClapdelete---No--+'
              '-Yes-'
```

Parámetros

nombre_admin_actual (Obligatorio)

Especifica el ID de usuario administrador cuyo nombre se ha de cambiar.

nombre_admin_nuevo (Obligatorio)

Especifica el nuevo ID de usuario administrador. La longitud máxima del nombre es de 64 caracteres.

SYNClapdelete

Especifica si desea suprimir el ID de usuario de administración en el servidor LDAP (Lightweight Directory Access Protocol) y sustituir el ID por uno nuevo.

Yes

Suprime el ID de usuario de administración en el servidor LDAP y lo sustituye por un ID nuevo.
Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

No suprime ni sustituye el ID de usuario de administración en el servidor LDAP. Este es el valor predeterminado.

Ejemplo: cambiar el nombre de un administrador

Redenominar el administrador de IBM Spectrum Protect CLAUDIA como BILL.

```
rename admin claudia bill
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME ADMIN

Mandato	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.

RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)

Utilice este mandato para redenominar un espacio de archivos de cliente existente en el servidor por un nuevo nombre de espacio de archivos o para redenominar espacios de archivos importados.

Puede que desee cambiar el nombre de un espacio de archivos que se ha importado o crear nuevos espacios de archivos activados para Unicode para clientes activados para Unicode.

Restricción: No cambie el nombre de los espacios de archivos NAS o VMware. Si cambia el nombre del espacio de archivos NAS o VMware, dejará de estar visible y no se puede restaurar. Para restaurar un espacio de archivos NAS o VMware renombrado, debe restablecer su nombre original y definir el parámetro force de la siguiente manera: force=yes

Clase de privilegio

Puede emitir este mandato un administrador con autorización de políticas ilimitada o con autorización de políticas limitada sobre el dominio de políticas del cliente.

Sintaxis

```
>>-REName Filespace--nombre_nodo----->
>--nombre_espacio_archivos_actual--nombre_espacio_archivos_nuevo-->
.-NAMEType----SERVER-----
>+-----+-----+----->
'-NAMEType----+SERVER--+'
      +-Unicode-+
      '-FSID----'

.-NEWNAMEType----SERVER-----
>+-----+-----+-----><
|                                     (1) | '-force----yes-'
'-NEWNAMEType----+Unicode-----+-'
      '-HEXadecimal-'
```

Notas:

1. Este parámetro es el valor predeterminado cuando se especifica NAMEType=Unicode.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente al que pertenece el espacio de archivos al que se le va a cambiar el nombre.

nombre_espacio_archivos_actual (Obligatorio)

Especifica el nombre del espacio de archivos que se ha de red denominar. Los nombres de espacios de archivos son sensibles a las mayúsculas y minúsculas y deben especificarse exactamente tal y como están definidos en el servidor. Se permite la utilización de nombres de asignación de espacio de archivos virtual.

nombre_espacio_archivos_nuevo (Obligatorio)

Especifica el nuevo nombre del espacio de archivos. Los nombres de espacios de archivos de cliente son sensibles a las mayúsculas y minúsculas y deben especificarse exactamente tal y como están definidos en el servidor. Este parámetro no puede ser un nombre de asignación de espacio de archivos virtual existente. Si `current_file_space_name` es un espacio de archivos virtual, `new_file_space_name` debe cumplir todas las reglas de definición de un nombre de espacio de archivos virtual. Consulte el mandato `DEFINE VIRTUALFSMAPPING` para obtener más información.

Importante: Si el nuevo tipo de nombre es hexadecimal, especifique valores hexadecimales UTF-8 válidos para que la página de códigos del servidor muestre el nombre del espacio de archivos como se pretende. Por ejemplo, no especifique un valor que puede interpretarse como un espacio de retroceso.

Cuando se cambia el nombre de un espacio de archivos que forma parte de un grupo de proximidad de espacio de archivos, el grupo de proximidad se actualiza con el nuevo nombre.

NAMEType

Especifique cómo desea que el servidor interprete el nombre de espacio de archivos actual que especifique. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS X y NetWare.

El valor predeterminado es `SERVER`. Si se especifica un nombre de asignación de espacio de archivos virtual, se debe utilizar `SERVER`. Los valores posibles son:

`SERVER`

El servidor utiliza la página de códigos del servidor para interpretar el nombre de espacio de archivos.

`Unicode`

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

`FSID`

El servidor interpreta el nombre de espacio de archivos como su identificador de espacio de archivos (FSID).

NEWNAMEType

Especifique cómo desea que el servidor interprete el nuevo nombre de espacio de archivos entrado. El valor predeterminado es `SERVER` si ha especificado el `NAMETYPE` como `SERVER`, o si el espacio de archivos que debe cambiarse de nombre no es Unicode. El valor predeterminado es `UNICODE` si ha especificado el `NAMETYPE` como `UNICODE`, o si el espacio de archivos que debe cambiarse de nombre es Unicode. Si se especifica un nombre de asignación de espacio de archivos virtual, se debe utilizar `SERVER`. Los valores posibles son:

`SERVER`

El servidor utiliza la página de códigos del servidor para interpretar el nombre de espacio de archivos.

`Unicode`

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Si la conversión no es satisfactoria, puede que desee especificar el parámetro `HEXADECIMAL`.

`HEXADECIMAL`

El servidor interpreta el nombre de espacio de archivo especificado como la representación hexadecimal de un nombre en Unicode. La utilización de la representación hexadecimal asegura que el servidor pueda red denominar correctamente el espacio de archivos, independientemente de la página de códigos del servidor.

Para visualizar la representación hexadecimal de un nombre de espacio de archivos, puede utilizar el mandato `QUERY FILESPACE` con `FORMAT=DETAILED`.

Restricción: No puede especificar un nombre de nuevo de un tipo que sea distinto del nombre original. Puede red denominar un espacio de archivos que es Unicode a otro nombre en Unicode. Puede red denominar un espacio de archivos que no es Unicode utilizando un nuevo nombre en la página de códigos del servidor. No puede mezclar los dos tipos.

force

Para renombrar un espacio de archivos NAS o VMware, debe establecer este parámetro de la siguiente manera: `force=yes`

[Cambiar el nombre de un espacio de archivos importado para evitar la sobregrabación](#)

Un nodo de cliente de AIX denominado LARRY ha realizado la copia de seguridad del espacio de archivos /r033 en el servidor de IBM Spectrum Protect. El espacio de archivos se ha exportado a cinta y después se ha reimportado al servidor. Al importarse este espacio de archivos, se ha creado un nombre generado por el sistema, /r031, para éste, pues /r033 ya existía para el nodo de cliente LARRY.

Sin embargo, el nodo cliente LARRY ya tenía un espacio de archivos denominado /r031 cuya copia de seguridad no se había realizado y, por lo tanto, el servidor lo desconocía. A menos que se cambie el nombre del espacio de archivos importado, éste recubrirá el espacio de archivos /r031, pues el nombre del espacio de archivos que ha generado la función IMPORT es igual al nombre de un espacio de archivos del nodo de cliente LARRY que el servidor desconoce.

Utilice el siguiente mandato para cambiar el nombre del espacio de archivos importado /r031. El nuevo nombre, /imported-r033, identifica que el nuevo espacio de archivos es una imagen importada del espacio de archivos /r033.

```
rename file space larry /r031 /imported-r033
```

Cambiar el nombre del espacio de archivos para crear un espacio de archivos activado para Unicode

El cliente JOE está utilizando un cliente de IBM Spectrum Protect activado para Unicode en inglés. JOE ha hecho copia de seguridad de varios espacios de archivos grandes que no son Unicode que está activado en el almacenamiento del servidor. El espacio de archivos \\joe\c\$ contiene algunos archivos con nombres de archivos en japonés cuya copia de seguridad no puede realizarse en un espacio de archivos que no esté activado para Unicode. Puesto que los espacios de archivos son de gran tamaño, el administrador no desea convertir ahora todos los espacios de archivos de JOE en espacios de archivos activados para Unicode. El administrador solamente desea cambiar el nombre del espacio de archivos que no es Unicode, \\joe\c\$, de modo que la próxima copia de seguridad del espacio de archivos dé lugar a la creación de un nuevo espacio de archivos activado para Unicode. El nuevo espacio de archivos activado para Unicode permitirá que se efectúe correctamente una copia de seguridad los archivos en japonés.

Utilice el siguiente mandato para cambiar el nombre \\joe\c\$:

```
rename filespace joe \\joe\c$ \\joe\c$_old
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME FILESPACE

Mandato	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.

RENAME NODE (Cambiar el nombre de un nodo)

Utilice este mandato para cambiar el nombre de un nodo.

Si asigna un ID de nodo existente a otra persona, utilice el mandato UPDATE NODE para cambiar la contraseña.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- No cambie el nombre de un nodo para que coincida con un ID de usuario de administración existente. Si cambia el nombre de un nodo y este coincide con un ID de usuario de administración, podría darse un comportamiento imprevisto debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría pasar que la actualización de la contraseña fallase.

Restricciones:

- No es posible cambiar el nombre de un nodo NAS que tenga definido un transportador de datos correspondiente. Si el transportador de datos tiene rutas definidas, deben suprimirse primero.
- Si un nodo se configura para la réplica, no se puede renombrar.

Si cambia el nombre de un nodo por un nombre que tiene un administrador, el método de autenticación del administrador y el valor de SSLREQUIRED se actualizan para que coincidan con los del nodo. Cuando un nodo y un administrador comparten un nombre y cambia el método de autenticación del nodo o el valor SSLREQUIRED del nodo, los valores del administrador también cambian. Debe tener autorización de nivel de sistema para actualizar el método de autenticación del nodo o el valor SSLREQUIRED del nodo y también actualizar un administrador con el mismo nombre.

Clase de privilegio

Debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-REName Node--nombre_nodo_actual--nuevo_nombre_nodo----->
      .-SYNClapdelete---No-----
>--+-----+-----+-----><
      '-SYNClapdelete---+-No---+'
              '-Yes-'
```

Parámetros

nombre_nodo_actual (Obligatorio)

Especifica el nombre del nodo que debe cambiarse.

nombre_nodo_nuevo (Obligatorio)

Especifica el nuevo nombre del nodo. La longitud máxima es de 64 caracteres.

SYNClapdelete

Especifica si el nombre de nodo se suprime y se sustituye en el servidor LDAP (Lightweight Directory Access Protocol).

Sí

Especifica que el nombre de nodo se suprime y se sustituye.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que el nombre de nodo no se suprime ni se sustituye. Este es el valor predeterminado.

Ejemplo: cambiar el nombre de un nodo

Cambiar el nombre del nodo JOE por JOYCE.

```
rename node joe joyce
```

Ejemplo: Cambiar el nombre de un nodo que comparte un espacio de nombres con otros servidores

Cambie el nombre del nodo de JOYCE a JOE sin suprimir el nombre anterior de los servidores LDAP correspondientes.

```
rename node joyce joe
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME NODE

Mandato	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

Tareas relacionadas:

Gestión de los nodos de servidor de archivos de NAS

RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)

Utilice este mandato para cambiar el nombre de un script de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de operador, políticas, almacenamiento o sistema.

Sintaxis

```
>>-REName SCRIpt--nombre_script_actual--nombre_nuevo_script----<<
```

Parámetros

nombre_script_actual (Obligatorio)

Especifica el nombre del script que se va a red denominar.

nombre_script_nuevo (Obligatorio)

Especifica el nuevo nombre del script. El nombre puede contener hasta 30 caracteres.

Ejemplo: cambiar el nombre de un script

Redenominar SCRIPT1 con el nuevo nombre de script SCRIPT2.

```
rename script script1 script2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME SCRIPT

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

RENAME SERVERGROUP (Redenominar un grupo de servidores)

Utilice este mandato para redenominar un grupo de servidores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REName SERVERGroup--nombre_grupo_actual--nombre_nuevo_grupo-><
```

Parámetros

nombre_grupo_actual (Obligatorio)

Especifica el grupo de servidores que se red denomina.

nombre_grupo_nuevo (Obligatorio)

Especifica el nuevo nombre del grupo de servidores. La longitud máxima del nombre es de 64 caracteres.

Ejemplo: cambiar el nombre de un grupo de servidores

Redenominar el grupo de servidores WEST_COMPLEX como BIG_WEST.

```
rename servergroup west_complex big_west
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME SERVERGROUP

Mandato	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)

Utilice este mandato para cambiar el nombre de una agrupación de almacenamiento. Puede cambiar los nombres de agrupaciones de almacenamiento de forma que se utilicen los mismos nombres en un gestor de configuración y en sus servidores gestionados.

Al cambiar el nombre de una agrupación de almacenamiento, todos los administradores con privilegio de almacenamiento restringido para la agrupación de almacenamiento anterior retienen el privilegio de almacenamiento restringido para la agrupación de almacenamiento renombrada. Si la agrupación de almacenamiento renombrada se encuentra en una jerarquía de agrupaciones de almacenamiento, se conserva la jerarquía. Debe actualizar la clase de gestión o el grupo de copia para especificar el nuevo nombre de agrupación de almacenamiento como destino para los archivos.

Si hay procesos activos cuando se renombra una agrupación de almacenamiento, puede que se siga mostrando el nombre antiguo en los mensajes o consultas de esos procesos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REName STGpool--nombre_agrupación_actual--nuevo_nombre_agrupación-><
```

Parámetros

nombre_agrupación_actual (Obligatorio)

Especifica la agrupación de almacenamiento que se redenomina.

nombre_agrupación_nueva (Obligatorio)

Especifica el nuevo nombre de la agrupación de almacenamiento. La longitud máxima del nombre es de 30 caracteres.

Ejemplo: cambiar el nombre de una agrupación de almacenamiento




Redenominar la agrupación de almacenamiento STGPOOLA con el nombre STGPOOLB:

```
rename stgpool stgpoola stgpoolb
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RENAME STGPOOL

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

Utilice este mandato para reparar extensiones con duplicados eliminados en una agrupación de almacenamiento de contenedores de directorio. Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones de las que se ha hecho copia de seguridad en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.

Restricciones:

- Sólo puede emitir el mandato REPAIR STGPOOL si ya ha emitido el mandato PROTECT STGPOOL para hacer una copia de seguridad de datos en otra agrupación de almacenamiento en un servidor de destino de réplica o en el mismo servidor.
- Cuando repara una agrupación de almacenamiento de contenedores de directorio del servidor de réplica, el mandato REPAIR STGPOOL falla cuando se produce cualquiera de las condiciones siguientes:
 - El servidor de destino no está disponible.
 - La agrupación de almacenamiento de destino está dañada.
 - Se produce una parada de red.
- Cuando repara una agrupación de almacenamiento de contenedores de directorio de agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla cuando se produce cualquiera de las condiciones siguientes:
 - La agrupación de almacenamiento de copia de contenedor no está disponible.
 - La agrupación de almacenamiento de copia de contenedor está dañada.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis cuando el origen es el servidor de réplica

```
>>-REPAir STGPool--nombre_agrupación----->
. -SRCLOCation----Replserver-.
>+-----+-----+-----+----->
' -SRCLOCation----Replserver-'

. -MAXSESSions----1-----
>+-----+-----+-----+----->
' -MAXSESSions-----número_sesiones--'

. -Preview ---No----- . -Wait----No-----
>+-----+-----+-----+-----><
' -Preview-----+No--+-' ' -Wait-----+No--+-'
' -Yes-' ' -Yes-'
```

Sintaxis cuando el origen es una agrupación de almacenamiento en el mismo servidor

```
>>-REPAir STGPool--nombre_agrupación--SRCLOCation-----Local----->
.-Preview ----No----- .-Wait----No-----
>-----+-----+-----+-----+-----+-----><
'-Preview-----+No--+-' '-Wait-----+No--+-'
          '-Yes-'          '-Yes-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que contiene los datos que se deben reparar.

SRCLOCation

Especifica la ubicación de origen utilizada para reparar los datos. El valor predeterminado es REPLSERVER. Este parámetro sólo es necesario cuando la ubicación de origen está en el mismo servidor. Puede especificar uno de los siguientes valores:

Local

Especifica que los datos se reparan de agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.

Replserver

Especifica que los datos se reparan de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino.

MAXSESSions

Especifica el número máximo de sesiones de datos que pueden enviar datos a un servidor de destino. Este parámetro es opcional cuando repara datos de un servidor de réplica.

El valor que se especifique puede estar en el rango de 1 a 20. El valor predeterminado es 1. Si aumenta el número de sesiones, puede reparar más rápidamente la agrupación de almacenamiento.

Cuando establezca un valor para el parámetro MAXSESSIONS, asegúrese de que el ancho de banda disponible y la capacidad del procesador de los servidores de origen y de destino sean suficientes.

Consejos:

- Si emite un mandato QUERY SESSION, el número total de sesiones puede superar el número de sesiones de datos.
- El número de sesiones que se utilizan para reparar agrupaciones de almacenamiento depende de la cantidad de datos que se reparan. Si está reparando solamente una cantidad pequeña de datos, no conseguirá ninguna ventaja si aumenta el número de sesiones.

Preview

Especifica si se van a previsualizar los datos o si se van a reparar. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que los datos se reparan en la agrupación de almacenamiento pero que no se previsualizan.

Yes

Especifica que los datos se previsualizan pero que no se reparan.

Wait

Especifica si se debe esperar a que el servidor termine el proceso de reparación de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar este parámetro solamente desde una línea de mandatos administrativa. Puede especificar uno de los siguientes valores:

No

Especifica que el mandato se procesa en segundo plano. Para supervisar el proceso en segundo plano del mandato REPAIR STGPOOL, emita el mandato QUERY PROCESS.

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

Ejemplo: reparar una agrupación de almacenamiento y obtener una vista previa de los datos

Reparar una agrupación de almacenamiento que se denomina POOL1 y previsualizar los datos.

```
repair stgpool pool1 preview=yes
```

Ejemplo: Reparar una agrupación de almacenamiento y especificar un número máximo de sesiones

Reparar una agrupación de almacenamiento que se denomina POOL1 y especificar un máximo de 10 sesiones.

```
repair stgpool pool1 maxsessions=10
```

Ejemplo: reparar una agrupación de almacenamiento desde cinta

Reparar una agrupación de almacenamiento llamada POOL1 y especificar local para la ubicación de origen.

```
repair stgpool pool1 SRCLOCATION=local
```

Tabla 1. Mandatos relacionados con REPAIR STGPOOL

Mandato	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.

REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)

Utilice este mandato para replicar los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, o a grupos definidos de nodos de clientes.

Cuando emite este mandato, se inicia un proceso en el que los datos que pertenecen a los nodos de cliente especificados se replican según las reglas de réplica. Los archivos que ya no se almacenan en el servidor de réplica de origen pero que existen en el servidor de réplica de destino se suprimen durante este proceso.

Consejo: Evite conflictos en la gestión de ID administrativos y conjuntos de opciones de cliente identificando los ID y conjuntos de opciones que se replican en el servidor de destino y los ID y conjuntos de opciones que se gestionan en una configuración empresarial. No puede definir un ID de usuario administrativo para un nodo registrado si ya existe un ID administrativo para el mismo nodo.

Si se está ejecutando un proceso de réplica de nodos para un nodo de cliente especificado por este mandato, el nodo se omite y se inicia la réplica para otros nodos que estén activados para la réplica.

Una vez que se haya completado el proceso de réplica de nodo, se puede iniciar un proceso de recuperación en el servidor de réplica de destino. Los archivos sólo se recuperan si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores a la recuperación de archivos dañados y replicados.

Restricción: No puede utilizar el parámetro REPLRECOVERDAMAGED para agrupaciones de contenedores de directorios o agrupaciones de nubes.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	No especificado	NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.

Consejo: Cuando se emite el mandato QUERY PROCESS durante la réplica de nodos, la salida puede mostrar resultados imprevistos para el número de réplicas completadas. El motivo de ello, para fines de réplica de nodos, es que se considera que cada espacio de archivos contiene tres espacios de archivos lógicos:

- Uno para objetos de copia de seguridad
- Uno para objetos de archivado
- Uno para objetos gestionados por espacio

De forma predeterminada, el mandato QUERY PROCESS genera resultados para cada espacio de archivos lógico. Hay otros factores que también afectan a la salida del mandato QUERY PROCESS:

- Si un espacio de archivo tiene una regla de réplica establecida en NONE, el espacio de archivos no se incluye en el recuento de espacios de archivos que se están procesando.
- Si especifica tipos de datos en el mandato REPLICATE NODE, sólo esos tipos de datos se incluyen en el recuento de espacios de archivos que se están procesando, menos cualquier espacio de archivos excluido.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-,-----
      v                   |
>>-REPLicate Node-----+nombre_nodo-----+----->
                          '-nombre_grupo_nodos-'

```

```

      .-*-----
      >-----+----->
      |      |      |      |
      | (1) v      |      |      |
      |-----+-----nombre_espacio_de_archivos-----+-----|
      | .-,-----
      |

```

```

| V (2) |
'-----FSID-----+-----+-----+'

.-NAMEType-----SERVER-----
>+-----+-----+-----+-----+-----+----->
'-NAMEType-----+-----SERVER-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----UNIcode-----+
|          (2) |
+-----FSID-----+'

.-CODEType-----BOTH-----
>+-----+-----+-----+-----+-----+----->
'-CODEType-----+-----BOTH-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----UNIcode-----+
+-----NONUNIcode-----+'

.-DATATYPE-----ALl-----
>+-----+-----+-----+-----+-----+----->
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
+-----V-----+
'-DATATYPE-----+-----Al-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----BACKUP-----+
+-----BACKUPActive-----+
+-----ARCHive-----+
+-----SPACEManaged-----+'

.-PRIORITY-----ALL-----
>+-----+-----+-----+-----+-----+----->
'-PRIORITY-----+-----ALL-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----HIGH-----+
+-----NORMAL-----+'

.-MAXSESSions-----10-----
>+-----+-----+-----+-----+-----+----->
'-MAXSESSions-----+-----número_sesiones-----+'

.-Preview -----No-----
>+-----+-----+-----+-----+-----+----->
'-Preview-----+-----No-----+'
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
|                                     |
+-----LISTfiles-----+-----No-----+
'-Yes-----+-----LISTfiles-----+-----No-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----Yes-----+'

.-Wait-----No-----
>+-----+-----+-----+-----+-----+----->
'-Wait-----+-----No-----+' '-RECOVERDamaged-----+-----Yes-----+'
|                                     |                                     |
|                                     |                                     |
|                                     |                                     |
|                                     |                                     |
+-----Yes-----+' +-----No-----+
|                                     |                                     |
|                                     |                                     |
|                                     |                                     |
+-----Solo-----+'

.-FORCEREConcile-----No-----
>+-----+-----+-----+-----+-----+----->
'-FORCEREConcile-----+-----No-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----Yes-----+'

.-TRANSFERMethod-----Tcpi-----
>+-----+-----+-----+-----+-----+-----><
'-TRANSFERMethod-----+-----Tcpi-----+'
|                                     |
|                                     |
|                                     |
|                                     |
+-----Fasp-----+'
|          (3) |
+-----Fasp-----+'

```

Notas:

1. No mezcle los FSID (identificadores de espacio de archivos) y los nombres de espacio de archivos en el mismo mandato.
2. No especifique un FSID si utiliza caracteres comodín para el nombre del nodo de cliente.
3. Sistemas operativos Linux El parámetro TRANSFERMETHOD solo está disponible en sistemas operativos Linux x86_64 .

Parámetros

nombre_nodo o **nombre_grupo_nodos** (Necesario)
Especifica el nombre del nodo de cliente y del grupo definido de nodos de cliente cuyos datos van a replicarse. También puede especificar una combinación de nombres de nodos de cliente y nombres de grupos de nodos de cliente. Para especificar varios nombres de nodos de cliente o nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede

utilizar caracteres comodín con los nombres de nodos de cliente pero no con los nombres de grupos de nodos de cliente. Se comprueban las reglas de réplica de todos los espacios de archivos en los nodos de cliente especificados.

nombre_espacio_archivos o FSID

Especifica el nombre del espacio de archivos o el identificador del espacio de archivos (FSID) que se ha de replicar. Un nombre o FSID es opcional. Si no especifica un nombre o un FSID, todos los datos de todos los espacios de archivos de los nodos de cliente especificados son candidatos para la réplica.

nombre_espacio_de_archivos

Especifica el nombre del espacio de archivos que tiene datos que se van a replicar. Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos, emita el mandato QUERY FILESPACE. Cuando existan varios nombres, separe éstos mediante comas, sin espacios intercalados. Cuando especifique el nombre, puede utilizar caracteres comodín.

Es posible que un servidor que tiene clientes con espacios de archivos que están habilitados para Unicode tenga que convertir el nombre de espacio de archivos. Por ejemplo, puede que el servidor deba convertir un nombre de la página de códigos del servidor a Unicode. Para obtener información adicional, consulte el parámetro NAMETYPE. Si no especifica ningún nombre de espacio de archivos o si especifica un único carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

FSID

Especifica el identificador del espacio de archivos que se va a replicar. El servidor utiliza los FSID para encontrar los espacios de archivos que se deben replicar. Para determinar el FSID de un espacio de archivos, emita el mandato QUERY FILESPACE. Cuando existan varios FSID, sepárelos mediante comas, sin espacios intercalados. Si especifica un FSID, el valor del parámetro NAMETYPE debe ser FSID.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y que tienen sistemas operativos Windows, Macintosh OS X o NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente cualificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacio de archivos utilizando los identificadores de espacios de archivos.

CODETYPE

Especifica el tipo de espacios de archivos que se van a incluir en el proceso de réplica de nodos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Puede especificar uno de los siguientes valores:

UNICODE

Incluir espacios de archivos que solo están en Unicode.

NONUNICODE

Especifica espacios de archivos que no están en Unicode.

BOTH

Especifica todos los espacios de archivos independientemente del tipo de página de códigos.

DATATYPE

Especifica el tipo de datos que se van a replicar. Los datos se replican según la regla de réplica que se aplica al tipo de datos. Este parámetro es opcional. Puede especificar uno o varios tipos de datos. Si no especifica un tipo de datos, se replican todos los datos de copia de seguridad, archivado y gestionados por espacio. Cuando existan varios tipos de datos, sepárelos mediante comas, sin espacios intercalados. No puede utilizar caracteres comodín. Puede especificar uno de los siguientes valores:

ALL

Replica todos los datos de copia de seguridad, archivado y gestionados por espacio en un espacio de archivos según la regla asignada al tipo de datos. Por ejemplo, suponga que NODE1 tiene un único espacio de archivos. Se aplican las siguientes reglas de réplica:

- Las reglas de espacio de archivos de los datos de copia de seguridad y archivado en el espacio de archivos se establecen en ALL_DATA.
- La regla de espacio de archivos de los datos gestionados por espacio se establece en DEFAULT.
- La regla de nodo de cliente de los datos gestionados por espacio se establece en NONE.

Si emite `REPLICATE NODE NODE1 DATATYPE=ALL`, sólo se replican los datos de copia de seguridad y los datos de archivado.

BACKUP

Replica los datos de seguridad activos e inactivos en un espacio de archivos si la regla de réplica que se aplica es ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY o ACTIVE_DATA_HIGH_PRIORITY.

BACKUPActive

Replica sólo los datos de copia de seguridad activos en un espacio de archivos si la regla de réplica que se aplica es ACTIVE_DATA o ACTIVE_DATA_HIGH_PRIORITY.

ARCHive

Replica los datos de archivado solo en un espacio de archivos si la regla de réplica de control es ALL_DATA o ALL_DATA_HIGH_PRIORITY.

SPACEManaged

Replica sólo los datos gestionados por espacio en un espacio de archivos si la regla de réplica que se aplica es ALL_DATA o ALL_DATA_HIGH_PRIORITY.

PRIority

Especifica los datos que se replican basándose en la prioridad de la regla de réplica. Puede especificar uno de los siguientes valores:

All

Replica todos los datos en un espacio de archivos si la regla de réplica que se aplica es ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY o ACTIVE_DATA_HIGH_PRIORITY.

High

Replica sólo los datos en un espacio de archivos que tienen una regla de réplica aplicada igual a ALL_DATA_HIGH_PRIORITY o ACTIVE_DATA_HIGH_PRIORITY.

Normal

Replica sólo los datos en un espacio de archivos que tienen una regla de réplica aplicada igual a ALL_DATA o ACTIVE_DATA.

MAXSESSions

Especifica el número máximo permitido de sesiones de datos que se utilizan para enviar datos a un servidor de réplica de destino. Este parámetro es opcional. El rango de valores es de 1 a 99. El valor predeterminado es 10.

El aumento del número de sesiones puede mejorar el rendimiento de la réplica de nodos.

Cuando establece este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas al proceso de réplica. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de los siguientes factores:

- Otra actividad del sistema y IBM Spectrum Protect
- Los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan

Asegúrese de que están disponibles los puntos y las unidades de montaje suficientes para que los procesos de réplica de nodo se puedan completar. Cada sesión de réplica necesitará un punto de montaje en los servidores de réplica de origen y destino para los volúmenes de agrupación de almacenamiento. Si el tipo de dispositivo no es FILE, cada sesión necesitará también una unidad en los servidores de réplica de origen y destino.

Cuando establezca un valor para MAXSESSIONS, tenga en cuenta también el ancho de banda disponible y la capacidad del procesador de los servidores de réplica de origen y destino.

Consejo:

- El valor que especifica el parámetro MAXSESSIONS sólo se aplica a las sesiones de datos. Las sesiones de datos son sesiones en las que los datos se envían a un servidor de réplica de destino. No obstante, si emite un mandato QUERY SESSION, el número total de sesiones puede exceder el número de sesiones de datos. La diferencia se debe a las sesiones de control breves que se utilizan para consultar y configurar operaciones de réplica.
- El valor del parámetro MAXSESSIONS representa el número máximo permitido de sesiones. El número de sesiones que se utilizan para réplica depende de la cantidad de datos que se deben duplicar. Si sólo va a replicar una pequeña cantidad de datos, no conseguirá ninguna ventaja si aumenta el número de sesiones. El número total de sesiones podría ser menor que el valor especificado por el parámetro MAXSESSIONS.

Preview

Especifica si se obtiene una vista previa de los datos. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que los datos se replican en el servidor de destino, pero no se obtiene una vista previa de los datos.

Yes

Especifica que se obtiene una vista previa de los datos, pero no se replican. Si especifica PREVIEW=YES, solo se mostrarán los volúmenes que se deben montar físicamente, como los volúmenes de cinta. No se mostrarán los volúmenes asignados a agrupaciones de almacenamiento que tienen una clase de dispositivo de FILE.

Se muestra la siguiente información en la salida:

- Los nombres de los nodos de cliente cuyos datos se replicarán.
- El número de archivos que se replicarán o suprimirán.
- La cantidad estimada de tiempo que se necesitará para completar el proceso de réplica de nodo.
- Una lista de los volúmenes que se van a montar.
- Un resumen de la información sobre los datos replicados y dañados. El resumen lista el número de nodos, los espacios de archivos, archivos y bytes que se pueden recuperar durante un proceso de recuperación de réplica. El resumen se visualiza solo si se especifica RECOVERDAMAGED=YES o RECOVERDAMAGED=ONLY.

Si los datos de nodo de cliente especificados por el mandato REPLICATE NODE no se han duplicado nunca y se especifica PREVIEW=YES, el nodo y los espacios de archivo se definen automáticamente en el servidor de réplica de destino.

LISTfiles

Especifica si se listan los nombres de los archivos que se replicarán. Este parámetro es opcional. El valor predeterminado es NO. Si especifica este parámetro, significa que el parámetro WAIT se ha establecido en YES y no puede emitir el parámetro WAIT desde la consola de servidor.

Puede especificar uno de los siguientes valores:

No

Especifica que no se muestran los nombres de los archivos que se replicarán.

Yes

Especifica que se muestran los nombres de los archivos que se replicarán.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el mandato se procesa de forma subordinada. Para supervisar el proceso en segundo plano del mandato REPLICATE NODE, emita el mandato QUERY PROCESS.

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato. No se puede especificar WAIT=YES desde la consola del servidor.

RECOVERDamaged

Especifica si un proceso de recuperación se ha iniciado en un servidor de réplica de destino después de completar el proceso de réplica de nodo. Este parámetro es opcional y sustituye a cualquier valor que haya especificado para el parámetro RECOVERDamaged cuando haya definido o actualizado un nodo. Puede especificar uno de los siguientes valores:

Yes

Especifica se ha iniciado un proceso de réplica para recuperar archivos dañados, pero sólo si el valor para el parámetro del sistema REPLRECOVERDAMAGED es ON. Si el valor es OFF, no se han recuperado archivos dañados.

No

Especifica que los archivos dañados no se recuperan.

Only

Especifica que se ha iniciado un proceso de réplica para el único fin de recuperar archivos dañados, pero sólo si el valor del parámetro REPLRECOVERDAMAGED del sistema está en ON. Si el valor es OFF, no se han recuperado archivos dañados y recibe una notificación de que la recuperación no se ha iniciado.

Restricción: Si especifica una combinación no válida de valores y parámetros para la recuperación de archivos, la réplica se detiene y aparece un mensaje de error.

FORCEREconcile

Especifica si se deben comparar todos los archivos en el servidor de réplica de origen con los archivos en el servidor de réplica de destino y sincronizar las diferencias entre ellos. Antes de la V7.1.1, este comportamiento era el valor predeterminado para el proceso de réplica. Cuando está instalado IBM® Tivoli Storage Manager V7.1.1 o posterior en los servidores de réplica de origen y destino, se ejecuta automáticamente una reconciliación durante la réplica inicial. Después de la réplica inicial, puede utilizar este parámetro por los motivos siguientes:

- Para sincronizar los archivos en los servidores de réplica de origen y destino si son diferentes.
- Para sustituir archivos inactivos que se omitieron después de cambiar las reglas de réplica de ACTIVE_DATA a ALL_DATA.
- Para suprimir archivos inactivos del servidor de réplica de destino cuando cambia las reglas de réplica ACTIVE_DATA a ALL_DATA.
- Para asegurarse de que sólo replica datos activos cuando se utiliza la regla de réplica ACTIVE_DATA de forma que el servidor de réplica de destino sólo tiene archivos activos.
- Para resincronizar los archivos para que el servidor de réplica de destino tenga los mismos archivos que el servidor de réplica de origen si anteriormente ha utilizado o está utilizando actualmente las políticas en el servidor de réplica de destino para gestionar los archivos replicados.
- Para volver a sincronizar los archivos en los servidores de réplica de origen y destino, si la base de datos ha regresado a un momento anterior utilizando un método distinto al mandato DSMSERV RESTORE DB.
- Para volver a enlazar los archivos a la nueva clase de gestión en el servidor de réplica de destino si esta clase de gestión no existía cuando se replicaron los archivos. Debe utilizar las políticas que están definidas en el servidor de réplica de destino para gestionar los archivos replicados.

Recuerde: Cuando se asigna la regla ALL_DATA, solo se completa una reconciliación para archivos activos en el servidor de réplica de origen.

Este parámetro es opcional. Puede especificar uno de los siguientes valores:


No

Especifica que el proceso de réplica no fuerza una reconciliación para comparar todos los archivos en el servidor de réplica de origen con archivos en el servidor de réplica de destino. En su lugar, el proceso de réplica realiza un seguimiento de los cambios de archivos en el servidor de réplica de origen desde la última réplica y sincroniza estos cambios en el servidor de réplica de destino. NO es el valor predeterminado.

Yes

Especifica que el proceso de réplica fuerza una reconciliación para comparar todos los archivos en el servidor de réplica de origen con archivos en el servidor de réplica de destino y sincroniza los archivos en el servidor de réplica de destino con el servidor de réplica de origen.

Sistemas operativos LinuxTRANSFERMethod

 Sistemas operativos LinuxEspecifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN). Si especifica TRANSFERMETHOD=FASP, altera temporalmente cualquier parámetro TRANSFERMETHOD que haya especificado en los mandatos DEFINE SERVER o UPDATE SERVER.

Restricciones:

- Solo los datos almacenados en una agrupación de almacenamiento de contenedores de directorio se pueden transferir utilizando tecnología Aspera FASP. Los datos que no se almacenan en una agrupación de almacenamiento de contenedores de directorio se transfieren utilizando TCP/IP.
- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, la réplica de nodo falla.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.

Ejemplo: replicar los datos por tipo de datos y prioridad

Replique los datos de copia de seguridad activos de prioridad alta y los datos de archivado de prioridad alta que pertenecen a todos los nodos de cliente en el grupo PAYROLL.

```
replicate node payroll datatype=backupactive,archive priority=high
```

Ejemplo: replicar todos los datos que pertenecen a un nodo según las reglas de réplica asignadas

NODE1 tiene un único espacio de archivos. Se aplican las siguientes reglas de réplica:

- Reglas de espacio de archivos:
 - Datos de copia de seguridad: ACTIVE_DATA
 - Datos de archivado: DEFAULT
 - Datos gestionados por espacio: DEFAULT
- Reglas de nodos cliente
 - Datos de copia de seguridad: DEFAULT
 - Datos de archivado: ALL_DATA_HIGH_PRIORITY
 - Datos gestionados por espacio: DEFAULT
- Reglas de servidor:
 - Datos de copia de seguridad: ALL_DATA
 - Datos de archivado: ALL_DATA
 - Datos gestionados por espacio: NONE

```
replicate node node1 priority=all
```

Los datos de copia de seguridad activos en el espacio de archivos se replican con una prioridad normal. Los datos de archivado se replican con una prioridad alta. Los datos gestionados por espacio no se replican.




Ejemplo: Recuperar archivos dañados sin iniciar el proceso de réplica completo

Sin iniciar el proceso de réplica completo, recupere los archivos dañados en los nodos cliente del grupo PAYROLL. Asegúrese de que el valor del parámetro del sistema REPLRECOVERDAMAGED está encendido. Después, emita el siguiente mandato:

```
replicate node payroll recoverdamaged=only
```

Mandatos relacionados

Tabla 2. Mandatos relacionados con REPLICATE NODE

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE REPLNODE	Elimina un nodo de la réplica.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

REPLY (Permitir una petición para continuar el proceso)

Utilice este mandato y un número de identificación para informar al servidor de que ha finalizado una operación solicitada. No todas las peticiones de servidor requieren una respuesta. Este mandato sólo es necesario si el mensaje de petición indica específicamente que se necesita una respuesta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```
>>-REply--número_solicitud--+-----+-----><
                               '-LABEL--etiqueta_volumen-'
```

Parámetros

número_solicitud (Necesario)

Especifica el número de identificación de la petición.

LABEL

Especifica la etiqueta que se grabará en un volumen al responder a un mensaje originado por el proceso de un mandato LABEL LIBVOLUME. Este parámetro es opcional.

Ejemplo: responder a una petición

Responder a una petición de respuesta utilizando 3 como el número de petición.

```
reply 3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REPLY

Mandato	Descripción
CANCEL REQUEST	Cancela las peticiones pendientes de montaje de volúmenes.
QUERY REQUEST	Muestra información acerca de todas las peticiones de montaje pendientes.

RESET PASSEXP (restablecer caducidad de contraseña)

Utilice el mandato RESET PASSEXP para restablecer el período de caducidad de las contraseñas en el período de caducidad común para las contraseñas de administrador y de nodo de cliente. El mandato RESET PASSEXP no se aplica a las contraseñas que se almacenan en un servidor de directorios LDAP.

Restricción: No puede restablecer el período de caducidad de contraseña en el período de caducidad común con el mandato SET PASSEXP.

Utilice el mandato QUERY STATUS para visualizar el período de caducidad común de las contraseñas.

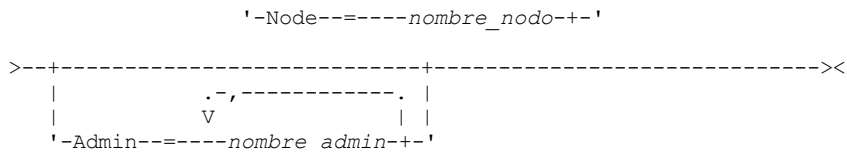
Restricción: Si no especifica el parámetro NODE o el parámetro ADMIN, se restablecerán los períodos de caducidad de contraseña para todos los nodos cliente y los administradores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-RESet PASSExp--+-----+----->
                    |           .-+-----+-----|
                    |           v                 |
```



Parámetros

Node

Especifica el nombre del nodo cuyo período de caducidad de contraseña quiere restablecer. Para especificar una lista de nodos, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Admin

Especifica el nombre del administrador cuyo período de caducidad de contraseña quiere restablecer. Para especificar una lista de administradores, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Ejemplo: restablecer el período de caducidad para nodos cliente específicos

Restablecer el período de caducidad de contraseña para los nodos cliente bj y katie.

```
reset passexp node=bj,katie
```

Ejemplo: restablecer la caducidad de contraseña para todos los usuarios

Restablecer los períodos de caducidad de contraseña para todos los usuarios en el período de caducidad común.

```
reset passexp
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RESET PASSEXP

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

RESTART EXPORT (Reiniciar una operación de exportación suspendida)

Utilice este mandato para reiniciar una operación de exportación suspendida.

Una operación de exportación se suspende cuando se detecta una de estas condiciones:

- Se emite un mandato SUSPEND EXPORT para la operación de exportación que está en ejecución.
- Operación realizada por adelantado: otro proceso ha suprimido el archivo que se va a leer para la exportación.
- Errores de comunicaciones en una exportación de servidor a servidor.
- No hay puntos de montaje disponibles.
- Los volúmenes necesarios no están disponibles.
- Se han encontrado errores de E/S.

Importante: Los nodos o espacios de archivos (en el servidor de exportación) en la operación de exportación original cuyos nombres se cambien con posterioridad no se incluirán en la operación resumida. Se suprimirán los demás datos para los nodos o los espacios de archivos del servidor de destino cuya supresión tiene lugar con anterioridad a la reanudación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-RESTART EXPORT .-*-----
+-----+-----<
'---identificador_exportación---'

```

Parámetros

identificador_exportación

Este parámetro opcional es el identificador exclusivo para la operación de exportación de servidor a servidor suspendida. Puede utilizar un carácter comodín para especificar este nombre. El nombre del identificador de exportación puede determinarse mediante la emisión del mandato QUERY EXPORT, que visualiza una lista de todas las operaciones de exportación de servidor a servidor actualmente suspendidas.

Ejemplo: reiniciar una exportación suspendida

Reiniciar la operación de exportación suspendida identificada mediante el nombre de mandato de exportación EXPORTALLACCTNODES.

```
restart export exportallacctnodes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RESTART EXPORT

Mandato	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

Mandatos RESTORE

Utilice los mandatos RESTORE para restaurar las agrupaciones de almacenamiento o volúmenes IBM Spectrum Protect.

- RESTORE NODE (Restaurar un nodo NAS)
- RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)
- RESTORE VOLUME (Restaurar datos de volumen primario desde una agrupación de copia o agrupación de datos activos)

RESTORE NODE (Restaurar un nodo NAS)

Utilice este mandato para iniciar una operación de restauración para un nodo de almacenamiento conectado a red (NAS).

Puede utilizar el mandato RESTORE NODE para restaurar las copias de seguridad que se han creado con el mandato del cliente BACKUP NAS o del mandato del servidor BACKUP NODE. Los datos NAS pueden restaurarse desde las agrupaciones de IBM Spectrum Protect nativas primarias o de copia, las agrupaciones NAS primarias o de copia o cualquier combinación necesaria para poder realizar la restauración.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el dominio al que está asignado el nodo o autorización de propietario de cliente en el nodo.

Sintaxis

```
>>-RESTORE Node--nombre_nodo--sistema_archivos_origen----->>
```



```

.-sistema_archivos_origen--.
>-----+----->
'-sistema_archivos_destino-'

>-----+----->
|               |               |
|               v               |
'-FILELIST-----+---nombre_archivo+-----+'
                '-FILE:--lista_archivos-'

.-NAMEType-----SERVER-----
>-----+----->
'-NAMEType-----+---SERVER-----+'
                +-HEXadecimal-+
                '-UNICODE-----'

.-PITDate-----TODAY-----
>-----+----->
'-PITDate-----+---mm/dd/aaa-----+'
                +-TODAY-----+
                +-TODAY-número_días-+
                '- número_días-----'

.-PITTime-----NOW----- .-Wait-----No-----
>-----+-----+----->
'-PITTime-----+---hh:mm:ss--+-' '-Wait-----+---No--+-'
                +-NOW-----+         '-Yes-'
                +-NOW-hh:mm-+
                '- hh:mm--'

.-TYPE-----BACKUPImage-----
>-----+-----><
'-TYPE-----+---BACKUPImage-+-'
                '-SNAPMirror--'

```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo que debe restaurarse. No es posible utilizar caracteres comodín ni una lista de nombres.

sistema_archivos_origen (Obligatorio)

Especifica el nombre del sistema de archivos que debe restaurarse. No es posible utilizar caracteres comodín en este nombre. No es posible especificar más de un sistema de archivos para su restauración. Se permite la utilización de nombres de espacio de archivos virtual.

sistema_archivos_destino

Especifica que el servidor de archivos restaura los datos en un sistema de archivos montado existente en el servidor de archivos. Este parámetro es opcional. El valor predeterminado es la ubicación original del sistema de archivos en el servidor de archivos. Se permite la utilización de nombres de espacio de archivos virtual.

FILELIST

Especifica la lista de nombres de archivos o directorios que han de restaurarse. Este parámetro es opcional. El valor predeterminado es la restauración de todo el sistema de archivos. Si se especifica este valor, el servidor intentará restaurar los objetos de la imagen adecuada. Si están especificados los parámetros PITDATE y PITTIME, el archivo se restaura desde la última imagen de copia de seguridad anterior al momento especificado. Si no están especificados los parámetros PITDATE y PITTIME, el archivo se restaura desde la última imagen de copia de seguridad del sistema de archivos.

Si la imagen es una copia de seguridad diferencial, los objetos se restauran primero desde la copia de seguridad completa correspondiente y, a continuación, desde la copia de seguridad diferencial. La restauración se realizará explorando las imágenes adecuadas para los objetos especificados y restaurando los que se encuentren. No se accede a las tablas de contenidos de estas imágenes, por lo que el servidor no comprueba si las imágenes contienen realmente los objetos.

La ruta de la carpeta y el nombre de archivo deben especificarse con barras inclinadas (/). No se necesitan barras inclinadas (/) de cierre al final del nombre de archivo. Todos los argumentos que contienen un espacio deben especificarse entre comillas dobles ("argument with spaces") de modo que engloben todo el argumento.

```
FILELIST="/path/to/nombre de archiv01 con espacios",/path/to/
nombre_archivo2_sin_espacios
```

En el caso de nombres de archivo que contengan comas, debe entrecomillarse todo el argumento con comillas dobles y simples ("argumento con comas").

```
FILELIST='"/path/to/nombearchivo1,con,comas"',/path/to/nombearchivo_sin_comas
```

Para restaurar un directorio completo, especifique un nombre de directorio en lugar de un nombre de archivo. Se restauran todos los archivos del directorio y los subdirectorios. No se necesita una barra inclinada (/) de cierre al final del nombre de directorio:

```
FILELIST=/path/to/mydir
```

nombre_archivo

Especifica uno o más nombres de archivos o directorios que han de restaurarse. Los nombres que especifique no pueden contener caracteres comodín. Los nombres deben separarse por comas y sin espacios intercalados. Los nombres de archivo son sensibles a las mayúsculas/minúsculas.

FILE:lista_archivos

Especifica el nombre de un archivo que contiene una lista de los nombres de archivos o directorios que han de restaurarse. En el archivo especificado, cada nombre de archivo o de directorio debe aparecer en una línea por separado. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo: Para restaurar los archivos FILE01, FILE02 y FILE03, cree un archivo llamado RESTORELIST que contenga una línea para cada archivo:

```
FILE01
FILE02
FILE03
```

Con el mandato, puede especificar los archivos que han de restaurarse de la forma siguiente:

```
FILELIST=FILE:RESTORELIST
```

NAMEType

Especifica cómo desea que el servidor interprete los nombres que ha especificado como FILELIST=nombre_archivo o los nombres que ha indicado en la lista del archivo que se ha especificado con FILELIST=lista_archivos. Este parámetro es útil cuando los nombres podrían contener caracteres Unicode. No tiene ningún efecto si no se ha especificado el parámetro FILELIST. El valor predeterminado es SERVER. Los valores posibles son:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres.

HEXadecimal

El servidor interpretará los nombres que se especifiquen como la representación hexadecimal de un nombre en Unicode. Para ver la representación hexadecimal de un nombre de archivo o de directorio, puede utilizar el mandato QUERY TOC con FORMAT=DETAILED.

UNICODE

El servidor interpretará los nombres como nombres con codificación UTF-8. Esta opción sólo se aplica cuando se ha especificado una lista con FILELIST=FILE:lista_archivos.

Restricción: El protocolo de gestión de datos de red (NDMP) tiene limitaciones que impiden que IBM Spectrum Protect informe acerca de si los archivos y directorios individuales se han restaurado correctamente o no.

PITDate

Especifica la fecha de instante específico. Cuando se utiliza con el parámetro PITTIME, PITDATE establece el instante específico a partir del cual desea seleccionar los datos que desea restaurar. Se restaurarán los datos más recientes de los que se ha hecho copia de seguridad hasta la fecha y hora especificadas. Este parámetro es opcional. El valor predeterminado es TODAY. Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	06/25/2001
TODAY	La fecha actual	TODAY
TODAY-días o bien -días	La fecha actual menos los días especificados	TODAY-7 o -7. Para restaurar datos de los que se ha hecho copia de seguridad hace una semana, especifique PITDATE=TODAY-7 o PITDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM

Valor	Descripción	Ejemplo
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

PITTime

Especifica la hora de instante específico. Cuando se utiliza con el parámetro PITDATE, PITTIME establece el instante específico a partir del cual desea seleccionar los datos que desea restaurar. Se restaurarán los datos más recientes de los que se ha hecho copia de seguridad hasta la fecha y hora especificadas. Este parámetro es opcional. El valor predeterminado es la hora actual. Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:33:28
NOW	La hora actual en la fecha especificada	NOW
NOW-HH:MM o bien -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30. Si emite este mandato a las 9:00 con PITTIME=NOW-03:30 o PITTIME=-03:30, el servidor restaurará registros de copia de seguridad cuya hora sea las 5:30 o posterior de la fecha de instante específico.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado. Utilice el mandato QUERY PROCESS para supervisar el proceso subordinado de este mandato.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

TYPE

Especifica el tipo de imagen que se ha de restaurar. El valor predeterminado para este parámetro es BACKUPIIMAGE y se utiliza para restaurar datos de copias de seguridad diferenciales o básicas NDMP estándares. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser específicos para un servidor de archivos determinado. Los valores posibles son:

BACKUPIImage

Especifica que debe restaurarse el sistema de archivos a partir de las imágenes de las copias de seguridad estándares NDMP apropiadas. Es el método predeterminado para realizar una operación de restauración NDMP. Si utiliza el tipo BACKUPIIMAGE puede restaurar datos de copias de seguridad diferenciales y básicas, y datos en el nivel de archivo.

SNAPMirror

Especifica que debe restaurarse el sistema de archivos a partir de una imagen de NetApp SnapMirror. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos NetApp. Una imagen SnapMirror solo puede restaurarse en un sistema de archivos que se haya preparado como volumen de destino SnapMirror. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más detalles.

Después de recuperar una imagen SnapMirror y copiarla en un sistema de archivos de destino, IBM Spectrum Protect rompe la relación de SnapMirror creada por el servidor de archivos durante la operación. Una vez finalizada la restauración, el sistema de archivos de destino recupera el mismo estado que el del sistema de archivos original en el instante específico de la copia de seguridad.

Cuando defina el parámetro TYPE como SNAPMirror, tenga en cuenta las siguientes restricciones:

Restricciones:

- No puede especificar el parámetro FILELIST.
- Ni el *nombre_sistema_archivos_origen* ni el *nombre_sistema_archivos_destino* pueden ser un nombre de espacio de archivos virtual.
- Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM® N-Series.

Ejemplo: restaurar un directorio completo

Restaura todos los archivos y los subdirectorios del directorio /mydir.
restore node nasnode /myfs /dest filelist=/path/to/mydir

Ejemplo: restaurar datos de un sistema de archivos

Restaurar datos del sistema de archivos /vol/vol10 en el nodo NAS NAS1.
restore node nas1 /vol/vol10

Ejemplo: restaurar una copia de seguridad de nivel de directorio en la misma ubicación

Restaura la copia de seguridad del nivel del directorio a su ubicación original. El origen es el nombre de espacio de archivos virtual /MIKESDIR y no se ha especificado ningún destino.

```
restore node nas1 /mikesdir
```

Para este ejemplo y el siguiente ejemplo, se da por supuesto que las siguientes definiciones de espacio de archivos virtual existen en el servidor para el nodo NAS1.

VFS Name	Filesystem	Path
/mikesdir	/vol/vol2	/mikes
/TargetDirVol2	/vol/vol2	/tmp
/TargetDirVol1	/vol/vol1	/tmp

Ejemplo: restaurar una copia de seguridad de nivel de directorio en un sistema de archivos distinto

Restaurar la copia de seguridad del nivel de directorio a un sistema de archivos distinto conservando la ruta.

```
restore node nas1 /mikesdir /vol/vol0
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RESTORE NODE

Mandato	Descripción
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
QUERY TOC	Visualiza detalles sobre la tabla de contenido para una imagen de copia de seguridad especificada.

RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)

Utilice este mandato para restaurar archivos desde una o varias agrupaciones de almacenamiento de copia o agrupaciones de datos activos hasta una agrupación de almacenamiento primaria.

IBM Spectrum Protect restaura todos los archivos de agrupaciones de almacenamiento primarias que:

- Se han identificado como teniendo errores
- Residen en un volumen con modalidad de acceso DESTROYED

Restricción: No puede utilizar este mandato para agrupaciones de almacenamiento de contenedor. Utilice el mandato REPLICATE STGPOOL para proteger datos de las agrupaciones de almacenamiento de contenedor.

También puede utilizar este mandato para identificar los volúmenes que contienen archivos primarios dañados. Durante el proceso de restauración, se emite un mensaje para cada volumen de la agrupación de almacenamiento restaurada que contiene los archivos dañados que no están en caché. Utilice el mandato QUERY CONTENT para identificar los archivos primarios dañados de un volumen específico.

No puede restaurar una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Además de restaurar datos en las agrupaciones de almacenamiento primarias que tienen los formatos de datos NATIVE o NONBLOCK, este mandato también le permite restaurar datos en las agrupaciones de almacenamiento primarias que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento primaria debe tener el mismo formato de datos que la agrupación de almacenamiento de copia desde la que se restaurarán datos. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

Consejo: Para restaurar datos de nodo cliente NAS en agrupaciones de almacenamiento NAS, debe cambiar manualmente la modalidad de acceso de los volúmenes por DESTROYED con el mandato UPDATE VOLUME. No obstante, si está usando el gestor de recuperación ante siniestro, el archivo del plan contendrá la información que necesita el servidor para marcar de forma automática los volúmenes como DESTROYED.

Puede que la restauración de archivos no sea completa si, durante el proceso de restauración, otros procesos de IBM Spectrum Protect han traspasado o suprimido datos activos o copias de archivos de copias de seguridad de agrupaciones de almacenamiento de copia. Para que no se produzca este problema, no emita los siguientes mandatos para copiar volúmenes de agrupación de almacenamiento de copia o de agrupación de datos activos mientras el proceso de restauración está en progreso:

- MOVE DATA
- DELETE VOLUME (DISCARDDATA=YES)
- AUDIT VOLUME (FIX=YES)

Asimismo, puede impedir la ejecución del proceso de reclamación de las agrupaciones de almacenamiento de copia estableciendo el porcentaje de RECLAIM en 100 con el mandato UPDATE STGPOOL.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento primaria para la que se han de restaurar los archivos. Si es usted un administrador con privilegio de almacenamiento con restricciones y desea restaurar archivos en una nueva agrupación de almacenamiento primaria, debe tener también autorización sobre la nueva agrupación de almacenamiento.

Sintaxis

```
>>-RESTORE STGpool--nombre_agrupación_primaria----->
>--+-----+----->
' -COPYstgpool----nombre_agrupación_copia-'
. -ACTIVEDATAOnly----No-----
>--+-----+----->
' -ACTIVEDATAOnly----+No-----+'
          '-Yes--| A |- '
>--+-----+----->
' -NEWstgpool----nombre_nueva_agrupación_primaria-'
. -MAXPRocess----1----- . -Preview ----No-----
>--+-----+----->
' -MAXPRocess----número-' ' -Preview----+No----+'
          '-Yes-'
. -Wait----No-----
>--+-----+----->>
' -Wait----+No----+'
          '-Yes-'

A (Yes)

|--ACTIVEDATAPool----nombre_agrupación_datos-activos-----|
```

Parámetros

nombre_agrupación_primaria (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento primaria que se está restaurando.

COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia desde la que se han de restaurar los archivos. Este parámetro es opcional. Si no se especifica este parámetro, se restaurarán los archivos desde cualquier agrupación de copia en la

que se puedan ubicar copias. No utilice este parámetro con los parámetros `ACTIVEDATAONLY` o `ACTIVEDATAPOOL`.

`ACTIVEDATAOnly`

Especifica que las versiones activas de archivos de copias de seguridad deben restaurarse únicamente a partir de las agrupaciones de datos activos. Este parámetro es opcional. El valor predeterminado es `NO`. Si no se especifica este parámetro, los archivos se restaurarán desde las agrupaciones de almacenamiento de copia. No utilice este parámetro con el parámetro `COPYSTGPOOL`. Los valores posibles son:

No

Especifica que la agrupación de almacenamiento no se restaurará desde las agrupaciones de datos activos.

Yes

Especifica que la agrupación de almacenamiento se restaurará desde la agrupación o agrupaciones activas que se especifiquen con el parámetro `ACTIVEDATAPOOL`. Si especifica el valor `YES` para `ACTIVEDATAONLY`, pero no especifica un valor para `ACTIVEDATAPOOL`, los archivos se restaurarán desde cualquier agrupación de datos activos en la que puedan localizarse versiones activas de los archivos de copia de seguridad.

Atención: La restauración de una agrupación de almacenamiento primaria desde una agrupación de datos activos podría dar lugar a que algunos o todos los archivos inactivos se supriman de la base de datos si el servidor determina que existe un archivo inactivo que debe sustituirse pero no puede encontrarlo en la agrupación de datos activos.

`ACTIVEDATAPool`

Especifica el nombre de la agrupación de datos activos desde la que se deben restaurar las versiones activas de archivos de copias de seguridad. Este parámetro es opcional. Si no se especifica este parámetro, los archivos se restaurarán desde cualquier agrupación de datos activos en la que se puedan ubicar versiones activas de archivos de copias de seguridad.

`NEWstgpool`

Especifica el nombre de la nueva agrupación de copia en la que se restaurarán los archivos. Este parámetro es opcional. Si no se especifica este parámetro, se restaurarán los archivos en la agrupación de almacenamiento primaria original (la agrupación que está restaurándose).

`MAXPRocess`

Especifica el número máximo de procesos paralelos que se utilizan para restaurar archivos. Al utilizar varios procesos paralelos, se puede mejorar el rendimiento de la operación de restauración. Este parámetro es opcional. Puede especificar un valor entre 1 y 999. El valor predeterminado es 1.

Al determinar este valor, tenga en cuenta el número de puntos de montaje (unidades lógicas) y de unidades físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es `FILE`, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la operación de restauración.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia y, si el tipo de dispositivo no es `FILE`, también necesita una unidad. Si efectúa la operación de restauración de archivos en una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si la clase de dispositivo no es `FILE`, una unidad adicional. Por ejemplo, imaginemos que especifica un máximo de 3 procesos para restaurar una agrupación de almacenamiento secuencial primaria desde una agrupación de almacenamiento de copia que tiene la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo 6 puntos de montaje y 6 unidades.

Para previsualizar una restauración, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

`Preview`

Especifica si se desea previsualizar la restauración sin hacerla. La función de previsualización permite identificar los volúmenes necesarios para restaurar la agrupación de almacenamiento. La función de previsualización muestra:

- Una lista de volúmenes de agrupación de almacenamiento primaria que contienen archivos dañados.
- El número de archivos y el número de bytes que se restaurarán, suponiendo que la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia necesarios es `READWRITE` o `READONLY`, cuando se realiza la operación de restauración.
- Una lista de los volúmenes de agrupación de almacenamiento de copia que contienen los archivos que se restaurarán. Estos volúmenes deben montarse si ejecuta la restauración.
- Una lista de todos los volúmenes que contienen archivos que no se pueden restaurar.

Nota: Para ver una lista de los volúmenes de agrupación de almacenamiento de copia fuera del local que se montarán durante una operación de restauración, cambie la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia a `UNAVAILABLE`. De este modo se evita el proceso de reclamación y de traspaso de datos de los volúmenes hasta que éstos se trasladan al local para efectuar la restauración.

Este parámetro es opcional. El valor predeterminado es `NO`. Los valores posibles son:

- No
Especifica que se realiza la operación de restauración.
- Yes
Especifica que se desea previsualizar la restauración sin llevarla a cabo realmente.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

- No
Especifica que el servidor procesa este mandato en un proceso subordinado.
Puede continuar trabajando con otras tareas mientras se procesa el mandato.
Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes. Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si cancela este proceso, pueden haberse restaurado ya algunos archivos antes de la cancelación.
- Yes
Especifica que el servidor realiza esta operación en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando la operación finaliza.
Nota: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: restaurar archivos desde una agrupación de almacenamiento de copia hasta la agrupación de almacenamiento primaria

Restaurar archivos de cualquier agrupación de almacenamiento de copia en la agrupación de almacenamiento primaria, PRIMARY_POOL.

```
restore stgpool primary_pool
```

Ejemplo: restaurar archivos desde una agrupación de datos activos específica hasta la agrupación de almacenamiento primaria

Restaurar archivos desde la agrupación de datos activos ADP1 hasta la agrupación de almacenamiento primaria PRIMARY_POOL.

```
restore stgpool primary_pool activedataonly=yes activedatapool=adp1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RESTORE STGPOOL

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

RESTORE VOLUME (Restaurar datos de volumen primario desde una agrupación de copia o agrupación de datos activos)

Utilice este mandato para restaurar todos los archivos que están en volúmenes dañados de una agrupación de almacenamiento primaria cuya copia de seguridad se ha realizado en una agrupación de almacenamiento de copia o en una agrupación de datos activos. IBM Spectrum Protect no restaura las copias en caché de los archivos y elimina de la base de datos esos archivos en caché durante el proceso de restauración.

Además de restaurar datos en los volúmenes de las agrupaciones de almacenamiento que tienen los formatos de datos NATIVE o NONBLOCK, este mandato también le permite restaurar datos en los volúmenes de las agrupaciones de almacenamiento que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). Los volúmenes que se desean restaurar deben tener el mismo formato de datos que los volúmenes de la agrupación de almacenamiento de copia. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

Este mandato cambia la modalidad de acceso de los volúmenes especificados a DESTROYED. Cuando se han restaurado todos los archivos de los volúmenes en otras ubicaciones, el volumen destruido estará vacío y se suprimirá de la base de datos.

La operación de restauración puede quedar incompleta debido a una o más de las razones siguientes:

- Nunca se efectuó una copia de seguridad de los archivos o las copias de seguridad están marcadas como dañadas. Utilice el mandato QUERY CONTENT para obtener más información acerca de los demás archivos del volumen.
- Se ha especificado una agrupación de almacenamiento de copia en el mandato RESTORE, pero se ha realizado la copia de seguridad de los archivos en una agrupación de almacenamiento de copia distinta. Utilice el parámetro PREVIEW cuando vuelva a emitir el mandato RESTORE para determinar si este es el problema.
- Los volúmenes de la agrupación de almacenamiento de copia que son necesarios para realizar una operación de restauración están fuera del local o no están disponibles. Compruebe en las anotaciones de actividades si se han producido mensajes durante el proceso de restauración.
- Otros procesos han traspasado o suprimido copias de seguridad de los archivos de agrupaciones de almacenamiento de copia durante el proceso de restauración. Consulte la nota 3.
- Se ha especificado una agrupación de datos activos para la restauración y no había archivos inactivos para realizar la copia.

Importante:

1. No puede restaurar volúmenes en agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.
2. Para poder restaurar un volumen de acceso aleatorio, primero debe emitir el mandato VARY para desactivar el volumen.
3. Para impedir que otros procesos traspasen o supriman archivos de agrupación de almacenamiento de copia, no emita los mandatos siguientes para los volúmenes de agrupación de almacenamiento de copia durante una operación de restauración:
 - MOVE DATA
 - DELETE VOLUME (DISCARDATA=YES)
 - AUDIT VOLUME (FIX=YES)

Para impedir el proceso de reclamación de las agrupaciones de almacenamiento de copia, emita el mandato UPDATE STGPOOL con el parámetro RECLAIM establecido en 100.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento restringido para la agrupación de almacenamiento primaria. Si es usted un administrador con privilegio restringido y desea restaurar archivos en una nueva agrupación de almacenamiento primaria, también debe tener autorización sobre la nueva agrupación de almacenamiento.

Sintaxis

```

      .-|-----|
      v      |
>>-RESTORE Volume----nombre_volumen+----->
>+-----+----->
' -COPYstgpool----nombre_agrupación_copia-'
      .-ACTIVEDATAOnly----No-----
>+-----+----->
' -ACTIVEDATAOnly----+No-----+-'
      ' -Yes--| A |- '
>+-----+----->
' -NEWstgpool----nombre_nueva_agrupación_primaria-'
      .-MAXProcess----1----- .-Preview ----No-----
>+-----+-----+----->
' -MAXProcess----número-' ' -Preview----+No----+'
      ' -Yes-'
```



```

.-Wait---No-----
>--+-----+-----><
'-Wait---+No--+-'
      '-Yes-'

```

A (Yes)

```
|--ACTIVEDATAPool-----nombre_agrupación_datos-activos-----|
```

Parámetros

nombre_volumen (Necesario)

Especifica el nombre de la agrupación de almacenamiento primaria que se restaura. Para especificar una lista de volúmenes que pertenecen a la misma agrupación de almacenamiento primaria, debe separar los nombres con comas y sin espacios intercalados.

COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia desde la que se han de restaurar los archivos. Este parámetro es opcional. Si no especifica este parámetro, se restaurarán los archivos desde todas las agrupaciones de copia en las que se puedan ubicar copias. No utilice este parámetro con los parámetros ACTIVATEDATAONLY o ACTIVATEDATAPOOL.

ACTIVEDATAOnly

Especifica que las versiones activas de archivos de copias de seguridad deben restaurarse únicamente a partir de las agrupaciones de datos activos. Este parámetro es opcional. El valor predeterminado es NO. Si no se especifica este parámetro, los archivos se restaurarán desde las agrupaciones de almacenamiento de copia. No utilice este parámetro con el parámetro COPYSTGPOOL. Los valores posibles son:

No

Especifica que la agrupación de almacenamiento no se restaurará desde las agrupaciones de datos activos.

Yes

Especifica que la agrupación de almacenamiento se restaurará desde la agrupación o agrupaciones activas que se especifiquen con el parámetro ACTIVATEDATAPOOL. Si especifica el valor YES para ACTIVATEDATAONLY, pero no especifica un valor para ACTIVATEDATAPOOL, los archivos se restaurarán desde cualquier agrupación de datos activos en la que puedan localizarse versiones activas de los archivos de copia de seguridad.

Atención: La restauración de un volumen desde una agrupación de datos activos podría dar lugar a que algunos o todos los archivos inactivos se supriman de la base de datos si el servidor determina que existe un archivo inactivo que debe sustituirse pero no puede encontrarlo en la agrupación de datos activos.

ACTIVEDATAPOOL

Especifica el nombre de la agrupación de datos activos desde la que se deben restaurar las versiones activas de archivos de copias de seguridad. Este parámetro es opcional. Si no se especifica este parámetro, los archivos se restaurarán desde cualquier agrupación de datos activos en la que se puedan ubicar versiones activas de archivos de copias de seguridad.

NEWstgpool

Especifica el nombre de la nueva agrupación de copia en la que se restaurarán los archivos. Este parámetro es opcional. Si no especifica este parámetro, los archivos se restaurarán en la agrupación de almacenamiento primaria original.

MAXPProcess

Especifica el número máximo de procesos paralelos que se utilizan para restaurar archivos. El rendimiento puede mejorar con el uso de procesos paralelos. Este parámetro es opcional. Puede especificar un valor entre 1 y 999. El valor predeterminado es 1.

Al determinar este valor, tenga en cuenta el número de puntos de montaje (unidades lógicas) y de unidades físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la operación de restauración.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia. Si el tipo de dispositivo no es FILE, cada proceso necesita también una unidad. Si restaura una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si la clase de dispositivo no es FILE, una unidad adicional. Por ejemplo, suponga que especifica un máximo de tres procesos para hacer copia de seguridad de una agrupación de almacenamiento primaria secuencial en una agrupación de almacenamiento de copia de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo 6 puntos de montaje y 6 unidades.

Para previsualizar una copia de seguridad, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

Preview

Especifica si se desea previsualizar la restauración sin hacerla. Puede utilizar esta opción para identificar los volúmenes fuera del local necesarios para restaurar una agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que desea realizar la operación de restauración.

Yes

Especifica que desea previsualizar la operación de restauración, pero restaurando los datos.

Consejo: Si se va a previsualizar una operación de restauración para ver la lista de los volúmenes de agrupación de copia fuera del local que se han de montar, debe cambiar la modalidad de acceso de los volúmenes identificados a UNAVAILABLE. De este modo impedirá la reclamación y el proceso MOVE DATA de estos volúmenes hasta que se hayan transportado a la ubicación del local para su utilización en el proceso de restauración.

La función de previsualización muestra lo siguiente:

- El número de archivos y de bytes que se restaurarán, si la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia es READWRITE o READONLY, cuando se realiza la operación de restauración.
- Una lista de los volúmenes de agrupación de almacenamiento de copia que contienen los archivos que se restaurarán. Estos volúmenes deben montarse si ejecuta la restauración.
- Una lista de los volúmenes que contienen archivos que no se pueden restaurar.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este mandato en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el mandato CANCEL PROCESS. Si cancela este proceso, puede haberse hecho ya copia de seguridad de algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza.

Recuerde: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: restaurar archivos de datos del volumen primario

Restaurar los archivos almacenados en el volumen PVOL2 de la agrupación de almacenamiento primaria PRIMARY_POOL.

```
restore volume pvol2
```

Ejemplo: restaurar los archivos de datos del volumen primario de una agrupación de datos activos

Restaurar los archivos almacenados en el volumen VOL001 de la agrupación primaria PRIMARY_POOL desde la agrupación de datos activos ADP1.

```
restore volume vol001 activedataonly=yes activedatapool=adp1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con RESTORE VOLUME

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.

Mandato	Descripción
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.

Mandatos REVOKE

Utilice los mandatos REVOKE para revocar el acceso o los privilegios.

- REVOKE AUTHORITY (revocar autorización de administrador)
- REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)

REVOKE AUTHORITY (revocar autorización de administrador)

Utilice este mandato para revocar una o varias clases de privilegios de un administrador.

También puede utilizar este mandato para restringir el número de dominios de políticas para los que un administrador de política restringida dispone de autorización y el número de agrupaciones de almacenamiento para las que un administrador de almacenamiento restringido dispone de autorización.

Si utiliza el mandato REVOKE AUTHORITY sin los parámetros CLASSES, DOMAINS y STGPOLS, revocará todos los privilegios del administrador especificado.

Como mínimo un administrador debe tener privilegio de sistema; por lo tanto, si el administrador es el único que tiene privilegio de sistema, no puede revocar la autorización.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-REVoKe AUTHority--nombre_admin----->
>+-----+
|          .-,------. |
|          v          | |
|'-Classes-----+SYstem-----+--+'
|                   +-Policy-----+
|                   +-STorage-----+
|                   +-Operator-----+
|                   '-Node--| A |-+'
>+-----+
|          .-,------. |
|          v          | |
|'-DObains-----nombre_dominio+--+'
>+-----+<
|          .-,------. |
|          (1) v          | |
|'-STGpools-----nombre_agrupación+--+'
A
.-AUTHority----Access-----
|-----+
|'-AUTHority----+Access+--+'
|                   '-Owner--+'
>--+DObains----nombre_dominio+-----|
|'-NOde----node_name-----+'
```

Notas:

1. Si se omiten todos estos parámetros, se revocarán todos los privilegios de administrador de este administrador.

Parámetros

nombre_admin (Necesario)

Especifica el nombre del administrador cuyo privilegio de administración se va a revocar o reducir.

CLasses

Especifica una o más clases de privilegios de administración que se revocarán a un administrador. Puede especificar varias clases separando cada una con una coma.

System

Indica que se ha de revocar la autorización del sistema para este administrador. Si se especifica CLASSES=SYSTEM, no pueden especificarse otras clases, ni tampoco pueden especificarse los parámetros DOMAINS y STGPOOLS.

Policy

Indica que se ha de revocar el privilegio de política de este administrador. Para revocar todos los privilegios de políticas, especifique CLASSES=POLICY y no especifique el parámetro DOMAINS.

STorage

Indica que se ha de revocar el privilegio de almacenamiento para este administrador. Para revocar todos los privilegios de almacenamiento, especifique CLASSES=STORAGE y no especifique el parámetro STGPOOLS.

Operator

Indica que se ha de revocar el privilegio de operador de este administrador.

Node

Indica que se ha de revocar el privilegio de nodo para este usuario.

AUTHority

Indica el nivel de autorización que se revoca para un usuario con privilegio de nodo. Este parámetro es opcional.

Si un administrador ya tiene privilegio de sistema o de políticas para el dominio de políticas al que pertenece el nodo, este mandato no modificará el privilegio del administrador.

Los niveles de autorización posibles son:

Access

Indica que se revoca la autorización de acceso a cliente. Es el valor predeterminado si se ha especificado CLASSES=NODE.

Nota: Un nodo cliente puede establecer la opción REVOKEREMOTEACCESS para evitar que acceda un usuario con privilegio de nodo y autorización de acceso a cliente. Si un usuario con privilegio de nodo tiene autorización de propietario de cliente, o tiene privilegios de sistema o de políticas para el dominio de políticas al que pertenece el nodo, ese administrador podrá seguir accediendo al cliente de copia de seguridad/archivado de Web.

Owner

Indica que se revoca la autorización de propietario de cliente.

DOmains

Indica que desea revocar la autorización de acceso a cliente o de propietario de cliente de un administrador para todos los clientes del dominio de políticas especificado. Este parámetro no se puede utilizar con el parámetro NODE.

NOde

Indica que desea revocar la autorización de acceso a cliente o de propietario de cliente de un administrador para el nodo. Este parámetro no se puede utilizar con el parámetro DOMAIN.

DOmains

Cuando se utiliza con CLASSES=POLICY, especifica una lista de los dominios de política que un administrador de políticas con restricciones ya no puede gestionar. (El administrador tenía autorización para gestionar estos dominios hasta que se ha emitido el mandato REVOKE.) Este parámetro es opcional. Los elementos de la lista se separan con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Se ha revocado la autorización para todos los dominios que coinciden. Si se especifica DOMAINS, el parámetro CLASSES=POLICY es opcional.

STGpools

Especifica una lista de agrupaciones de almacenamiento que ya no puede gestionar un administrador con privilegio de política con restricciones. (El administrador tenía autorización para gestionar estas agrupaciones de almacenamiento hasta que se ha emitido el mandato REVOKE.) Este parámetro es opcional. Los elementos de la lista se separan con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Se revocará la autorización para todas las agrupaciones de almacenamiento que coincidan. Si se especifica STGPOOLS, entonces el parámetro CLASSES=STORAGE es opcional.

Notas de uso

1. Para que un administrador con privilegio de almacenamiento sin restricciones pase a tener privilegio de almacenamiento con restricciones, en primer lugar debe utilizar este mandato para revocar el privilegio sin restricciones. A continuación, ha de utilizar el mandato GRANT AUTHORITY para otorgar al administrador privilegio de almacenamiento con restricciones y para identificar las agrupaciones de almacenamiento sobre las que el administrador tiene autorización.

Para revocar el privilegio de política sin restricciones de un administrador, especifique el parámetro CLASSES=STORAGE. No puede utilizar el parámetro STGPools para revocar la autorización sobre las agrupaciones de almacenamiento seleccionadas de un administrador con privilegio de almacenamiento sin restricciones.

2. Para que un administrador con privilegio de política sin restricciones pase a tener privilegio de política con restricciones, en primer lugar debe utilizar este mandato para revocar el privilegio sin restricciones. A continuación, ha de utilizar el mandato GRANT AUTHORITY para otorgar al administrador privilegio de política con restricciones y para identificar los dominios de políticas sobre los que el administrador tiene autorización.

Para revocar el privilegio de política sin restricciones de un administrador, especifique el parámetro CLASSES=POLICY. No puede utilizar el parámetro DOMAINS para revocar la autorización sobre los dominios seleccionados de un administrador con privilegio sin restricciones.

Ejemplo: revocar determinados privilegios de administración

Revocar parte de los privilegios del administrador CLAUDIA. CLAUDIA tiene privilegio de política con restricciones para los dominios de políticas EMPLOYEE_RECORDS y PROG1. Limitar los privilegios de políticas de CLAUDIA al dominio de políticas EMPLOYEE_RECORDS.

```
revoke authority claudia classes=policy
domains=employee_records
```

Ejemplo: revocar todos los privilegios de administración

El administrador LARRY actualmente tiene privilegios de operador y de políticas con restricciones. Revocar todos los privilegios del administrador LARRY. Para revocar todos los privilegios de un administrador, identifique al administrador, pero no especifique CLASSES, DOMAINS o STGPools. LARRY continúa siendo un administrador pero únicamente podrá utilizar los mandatos que puede emitir cualquier administrador.

```
revoke authority larry
```

Ejemplo: revocar privilegio de nodo

El usuario de personal del departamento de soporte CONNIE tiene actualmente privilegio de nodo con autorización de propietario de cliente para el nodo cliente WARD3. Revocar su privilegio de nodo con autorización de propietario de cliente.

```
revoke authority connie classes=node
authority=owner node=ward3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REVOKE AUTHORITY

Mandato	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.

REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)

Utilice este mandato para revocar la autoridad de un nodo cliente agente para realizar operaciones de copia de seguridad y restauración para un nodo de destino en el servidor de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones

Sintaxis

```
>>-REVoKe PROXynode TArget---nombre_nodo_destino----->
>--AGent---nombre_nodo_agente-----<
```

Parámetros

TArget (Obligatorio)

Especifica el nodo de destino al cual ha otorgado autorización de proxy el nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.

AGent (Obligatorio)

Especifica qué nodo tiene autorización para actuar como proxy respecto al nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.

Ejemplo: revocar la autorización de proxy de un nodo

Para revocar la autorización del nodo de destino NASCLUSTER que actúa como proxy para todos los nodos agente que empiezan por la letra M, emita el mandato siguiente.

```
revoke proxynode target=nascluster agent=m*
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con REVOKE PROXYNODE

Mandato	Descripción
GRANT PROXYNODE	Concede autorización de proxy a un nodo agente.
QUERY PROXYNODE	Visualiza los nodos con autoridad para actuar como nodos proxy.

ROLLBACK (Retrotraer cambios no validados en una macro)

Utilice este mandato en una macro para deshacer todos los cambios de proceso que han realizado los mandatos que el servidor ha ejecutado pero que todavía no se han validado en la base de datos. Un cambio validado es permanente y no se puede retrotraer. El mandato ROLLBACK es útil para probar las macros.

Asegúrese de que su sesión de cliente de administración no está ejecutándose con la opción ITEMCOMMIT cuando utilice este mandato.

Importante: Los mandatos SETOPT en una macro no pueden retrotraerse.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-ROLLBACK-----<
```

Parámetros

Ninguno

Ejemplo: retrotraer cambios en una macro

Ejecute la macro REGN con el mandato ROLLBACK para verificar que la macro funciona sin validar ningún cambio. El contenido de la macro es :

```
/* Macro para registrar administradores
de políticas y otorgar autorización */
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
REGister Admin ken plane
```

```
Grant AUTHority ken CLasses=Policy
ROLLBACK /* impide que se validen los cambios */
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con ROLLBACK

Mandato	Descripción
COMMIT	Hace que los cambios en la base de datos sean permanentes.
MACRO	Ejecuta un archivo de macro especificado.

Conceptos relacionados:

Macros de cliente administrativo

RUN (ejecutar un script de IBM Spectrum Protect)

Utilice este mandato para ejecutar un script de IBM Spectrum Protect. Para emitir este mandato en otro servidor, el script que se ejecuta debe estar definido en ese servidor.

Puede incluir mandatos RUN en los scripts siempre que éstos no creen bucles. Por ejemplo, debe evitar incluir mandatos RUN donde SCRIPT_A ejecuta SCRIPT_B y SCRIPT_B ejecuta SCRIPT_A.

Importante: IBM Spectrum Protect no dispone de un mandato que pueda cancelar un script después de haberse iniciado éste. Para detener un script, debe detener el servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de operador, políticas, almacenamiento o sistema.

Sintaxis

```
>>-RUN--nombre_script--+-----+----->
      | .-,-----, |
      | V           | |
      '---valor_sustitución---'

.-Preview ----No----- .-Verbose-----No-----
>+-----+-----+-----+-----<
'-Preview-----+No--+-' '-Verbose-----+No--+-'
      '-Yes-'                '-Yes-'
```

Parámetros

nombre_script (Obligatorio)

Especifica el nombre del script que desea procesar. El nombre que especifique no puede ser una variable de sustitución como, por ejemplo, \$1.

substitution_value

Especifica uno o varios valores que se sustituirán por variables al ejecutarse el script. En un script, una variable de sustitución se compone de un carácter '\$' seguido de un número. Al ejecutar el script, IBM Spectrum Protect sustituye las variables de sustitución definidas en un script con los valores suministrados con este mandato. Debe especificar valores para cada una de las variables de sustitución definidas en el script; de lo contrario, el script no se ejecutará. Este parámetro es opcional.

Preview

Especifica si se previsualizan las líneas de mandatos del script sin ejecutar realmente el script. El valor predeterminado es NO. Los valores posibles son:

Yes

Especifica que se visualizan las líneas de mandatos incluidas en un script, pero el script no se procesa.

No

Especifica que se visualizan las líneas de mandatos incluidas en un script y el script se procesa.

Verbose

Especifica hay que visualizar las líneas de mandatos, la sustitución de variables y el recorrido por la lógica condicional a medida que se procesa el script. Este parámetro se ignora si se especifica PREVIEW=YES. El valor predeterminado es NO. Los valores posibles son:

Yes

Especifica que se visualicen las líneas de mandatos, la sustitución de variables y el recorrido de la lógica condicional a medida que se procesa el script.

No

Especifica que no se visualicen las líneas de mandatos, la sustitución de variables y el recorrido de la lógica condicional a medida que se procesa el script.

Ejemplo: ver los mandatos que ha generado un script con una variable de sustitución de nombre de tabla

Para ejecutar el siguiente script de ejemplo, denominado QSAMPLE, emita un mandato RUN que especifique el nombre de tabla ACTLOG como valor para la variable de sustitución, \$1. Utilice la salida para obtener una previsualización de los mandatos que genera el script antes de ejecutar los mandatos.

```
001 /* Esta es una consulta SQL con formato amplio */
005 SET SQLDISPLAYMODE WIDE
010 SELECT colname FROM -
015 COLUMNS WHERE TABNAME='$1'

run qsample actlog preview=yes

ANR1461I RUN: Ejecutando el script de mandatos QSAMPLE.
ANR1466I RUN: Script de mandatos QSAMPLE, Línea 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Script de mandatos QSAMPLE, Línea 15:
           select colname from columns where tabname='ACTLOG'.
ANR1470I RUN: Script de mandatos QSAMPLE completado correctamente
           (modo PREVIEW)
```

Ejemplo: ejecutar un script para que se visualicen y se ejecuten los mandatos que genera el script

Ejecutar el mismo script como se mostraba en el ejemplo anterior para que se visualicen los mandatos generados y los resultados de los mandatos.

```
run qsample actlog verbose=yes

ANR1461I RUN: Ejecutando el script de mandatos QSAMPLE.
ANR1466I RUN: Script de mandatos QSAMPLE, Línea 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Script de mandatos QSAMPLE, Línea 5: RC=RC_OK
ANR1466I RUN: Script de mandatos QSAMPLE, Línea 15:
           select colname from columns where tabname='ACTLOG'.

COLNAME
-----
DATE_TIME
MSGNO
SEVERITY
MESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Script de mandatos QSAMPLE, Línea 15: RC=RC_OK
ANR1462I RUN: Script de mandatos QSAMPLE completado correctamente.
```

Ejemplo: ejecutar un script para que sólo se visualicen los resultados de los mandatos del script

Ejecutar el script de ejemplo anterior, sin que se visualicen los mandatos generados, sólo los resultados de los mandatos generados en el script.

```
run qsample actlog verbose=no

COLNAME
-----
DATE_TIME
MSGNO
SEVERITY
MESSAGE
```


ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Script de mandatos QSAMPLE completado correctamente.

Mandatos relacionados

Tabla 1. Mandatos relacionados con RUN

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
UPDATE SCRIPT	Cambia o añade líneas a un script.

Tareas relacionadas:

Ejecución de un script del servidor

SELECT (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)

Utilice el mandato SELECT para crear y dar formato a una consulta personalizada de la base de datos de IBM Spectrum Protect .

IBM Spectrum Protect proporciona una interfaz SQL para un programa de DB2. DB2 maneja directamente las restricciones y las directrices para gestionar consultas SQL.

Como ayuda para encontrar la información que está disponible, IBM Spectrum Protect proporciona tres tablas de catálogos del sistema:

SYSCAT.TABLES

Contiene información acerca de todas las tablas que pueden consultarse con el mandato SELECT.

SYSCAT.COLUMNS

Describe las columnas de cada tabla.

Puede emitir el mandato SELECT para consultar estas tablas y determinar la ubicación de la información que desea obtener.

Notas de uso

No puede emitir el mandato SELECT desde una consola de servidor.

Dado que el mandato SELECT no bloquea ni desbloquea registros, la contención de un registro puede provocar que el servidor emita por error el mensaje ANR2034E: *SELECT: No se ha encontrado ninguna entrada con este criterio.* Compruebe que sus criterios de selección sean correctos y ejecute el mandato de nuevo.

Para detener el proceso de un mandato SELECT después de haberse iniciado éste, cancele la sesión de administración desde la que se ha emitido el mandato. Puede cancelar la sesión desde la consola del servidor o desde otra sesión de administración.

Los espacios de tabla temporales se utilizan para procesar consultas SQL en DB2. Un espacio temporal inadecuado puede provocar errores de consulta SQL.

Para exportar la salida de un archivo separado por comas para su importación a una hoja de cálculo, utilice las opciones de línea de mandatos -comma y > las opciones de línea de mandatos en el mandato dsmadm.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

Para obtener la sintaxis de la sentencia SELECT y las directrices, busque en Información sobre el producto DB2.

Importante: La sintaxis adecuada para la sentencia Select de la indicación de fecha y hora es:

```
SELECT * FROM SUMMARY WHERE ACTIVITY='EXPIRATION' AND START_TIME >'2009-05-10 00:00:00' AND START_TIME <'2009-05-11 23:23:23'
```

Lista de ejemplos

El mandato SELECT se utiliza para personalizar gran diversidad de consultas. Para darle una idea de lo que puede hacer con el mandato, esta sección incluye muchos ejemplos. Sin embargo, existen muchas más posibilidades. La salida de la consulta se muestra únicamente para los mandatos más complejos para poder ilustrar su formato.

En la lista siguiente se resumen los mandatos SELECT de ejemplo:

- Lista las contraseñas del ID de usuario administrador que se autentican con un servidor de directorios LDAP externo
- Obtener una lista de las tablas disponibles
- Obtener una lista de los nodos cliente y de los clientes de administración que actualmente tienen bloqueado el acceso al servidor
- Obtener una lista de los nodos cliente y de los clientes de administración que finalmente no han especificado la contraseña correcta
- Obtener una lista de los nodos del dominio de políticas estándar que no se han asociado a la planificación de copia de seguridad diaria DAILYBACKUP
- Obtener una lista de los administradores que disponen de autorización de política
- Obtener una lista de los mensajes de tipo E (ERROR) o W (WARNING) que se han emitido en el período de tiempo durante el cual han estado realizándose tareas de mantenimiento para los registros del registro de actividad
- Obtener una lista de las planificaciones de administración que ha definido o alterado el administrador JAKE
- Obtener una lista de las prioridades de planificación de administración relativas
- Obtener una lista de las clases de gestión que tienen un grupo de copias archivadas con un período de retención de más de 365 días
- Obtener una lista de los nodos cliente que se encuentran en cada dominio de políticas
- Contar el número de archivos que se han archivado de cada nodo
- Obtener una lista de los clientes que utilizan la gestión de espacio
- Determinar cuántos volúmenes deberían reclamarse si el umbral de reclamación se cambia al 50 para la agrupación de almacenamiento TAPE
- Determinar cuántos archivos de copia de seguridad se verían afectados en cada nodo si se cambiara o suprimiera la clase de gestión DAILY en el dominio de políticas STANDARD
- Para todas las sesiones de cliente activas, determinar durante cuánto tiempo han estado conectadas éstas y su rendimiento efectivo en bytes por segundo
- Determinar durante cuánto tiempo han estado ejecutándose los procesos en segundo plano actuales y determinar su rendimiento efectivo en términos de tiempo y de archivos por segundo
- Contar el número de nodos cliente que existen para cada tipo de plataforma
- Contar el número de espacios de archivos que tiene cada nodo y obtener una lista de los nodos cliente por orden ascendente
- Obtener información estadística para calcular el número de volúmenes fuera del local cuyo espacio se reclama durante la reclamación de una agrupación de almacenamiento.
- Obtener registros de detalle de estimaciones de PVU
- Obtener información sobre los roles del nodo
- Obtener información sobre el estado.

Ejemplo: Lista los ID de usuario administrador que se autentican con el servidor IBM Spectrum Protect

Lista todos los ID de usuario administrador cuyas contraseñas se autentican con el servidor IBM Spectrum Protect :

```
select admin_name from admins where authentication=local
```

Ejemplo: obtener una lista de las tablas disponibles

Obtener una lista de todas las tablas disponibles para consultar la base de datos de IBM Spectrum Protect.

```
select * from syscat.tables  
  
ABSHEMA: SERVER1  
TABNAME: ACTLOG  
CREATE_TIME: 1999-05-01 07:39:06  
COLCOUNT: 10
```

```

INDEX_COLCOUNT: 1
UNIQUE_INDEX: FALSE
REMARKS: Server activity log

TABSHEMA: SERVER1
TABNAME: ADMIN_SCHEDULES
CREATE_TIME: 1995-05-01 07:39:06
COLCOUNT: 14
INDEX_COLCOUNT: 1
UNIQUE_INDEX: TRUE
REMARKS: Administrative command schedules

TABSHEMA: SERVER1
TABNAME: ADMINS
CREATE_TIME: 1995-05-01 07:39:06
COLCOUNT: 15
INDEX_COLCOUNT: 1
UNIQUE_INDEX: TRUE
REMARKS: Server administrators

TABSHEMA: SERVER1
TABNAME: ARCHIVES
CREATE_TIME: 1995-05-01 07:39:06
COLCOUNT: 10
INDEX_COLCOUNT: 5
UNIQUE_INDEX: FALSE
REMARKS: Copias archivadas cliente

```

Ejemplo: obtener una lista de los nodos cliente y de los clientes de administración que actualmente tienen bloqueado el acceso al servidor

```

select node_name from nodes where locked='YES'

select admin_name from admins where locked='YES'

```

Ejemplo: listar nodos de cliente, clientes administrativos y servidores que están utilizando la seguridad de sesión transicional

```

select node_name from nodes where session_security='Transitional'

select admin_name from admins where session_security='Transitional'

select server_name from servers where session_security='Transitional'

```

Ejemplo: obtener una lista de los nodos cliente y de los clientes de administración que finalmente no han especificado la contraseña correcta

```

select node_name from nodes where invalid_pw_count <>0

select admin_name from admins where invalid_pw_count <>0

```

Ejemplo: obtener una lista de los nodos del dominio de políticas estándar que no se han asociado a la planificación de copia de seguridad diaria DAILYBACKUP

```

select node_name from nodes where domain_name='STANDARD' and
node_name not in (select node_name from associations
where domain_name='STANDARD' and
schedule_name='DAILYBACKUP')

```

Ejemplo: listar los administradores que disponen de autorización de política

```

select admin_name from admins where
upper(system_priv) <>'NO'
or upper(policy_priv) <>'NO'

```

Ejemplo: obtener una lista de los mensajes de tipo E (ERROR) o W (WARNING) que se han emitido en el período de tiempo durante el cual han estado realizándose tareas de mantenimiento para los registros del registro de actividad

```
select date_time,msgno,message from actlog
where severity='E' or severity='W'
```

Ejemplo: obtener una lista de las planificaciones de administración que ha definido o alterado el administrador JAKE

```
select schedule_name from admin_schedules
where chg_admin='JAKE'
```

Ejemplo: obtener una lista de las prioridades de planificación de administración relativas

```
select schedule_name,priority from admin_schedules order
by priority
```

Ejemplo: obtener una lista de las clases de gestión que tienen un grupo de copias archivadas con un período de retención de más de 365 días

```
select domain_name,set_name,class_name from ar_copygroups
where retver='NOLIMIT' or cast(retver as integer) >365
```

Ejemplo: obtener una lista de las clases de gestión que especifican más de cinco versiones de copia de seguridad

```
select domain_name,set_name,class_name from bu_copygroups
where verexists = 'NOLIMIT' or
cast(verexists as integer)>5
```

Ejemplo: obtener una lista de los nodos cliente que utilizan el conjunto de opciones de cliente denominado SECURE

```
select node_name from nodes where option_set='SECURE'
```

Ejemplo: obtener una lista de los nodos cliente que se encuentran en cada dominio de políticas

```
select domain_name,num_nodes from domains
```

Ejemplo: contar el número de archivos que se han archivado de cada nodo

Atención: Este mandato puede tardar mucho tiempo en finalizar.

```
select node_name,count(*) from archives
group by node_name
```

Ejemplo: obtener una lista de los clientes que utilizan la gestión de espacio

```
select node_name from auditocc where spacemg_mb <>0
```

Ejemplo: determinar cuántos volúmenes deberían reclamarse si el umbral de reclamación se cambia al 50 para la agrupación de almacenamiento TAPE

```
select count(*) from volumes where stgpool_name='TAPE'
and upper(status)='FULL' and pct_utilized < 50
```

Ejemplo: determinar cuántos archivos de copia de seguridad se verían afectados en cada nodo si se cambiara o suprimiera la clase de gestión DAILY en el dominio de políticas STANDARD

Nota: Este mandato necesita una cantidad de tiempo y de recursos significativa para completarse.

```
select node_name, count(*) as "Files" from backups
where class_name='DAILY' and node_name in
(select node_name from nodes where domain_name='STANDARD')
group by node_name
```

Ejemplo: para todas las sesiones de cliente activas, determinar durante cuánto tiempo han estado conectadas éstas y su rendimiento efectivo en bytes por segundo

```

select session_id as "Sesión",
client_name as "Cliente",
state as "Estado",
current_timestamp-start_time as "Tiempo transcurrido",
(cast(bytes_sent as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes enviados/segundo",
(cast(bytes_received as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes recibidos/segundo"
from sessions

```

```

Sesión: 24
Cliente: ALBERT
Estado: Run
Tiempo transcurrido: 0 01:14:05.000000
Bytes enviados/segundo: 564321,9302768451
Bytes recibidos/segundo: 0,0026748857944

```

```

Sesión: 26
Cliente: MILTON
Estado: Run
Tiempo transcurrido: 0 00:06:13.000000
Bytes enviados/segundo: 1638,5284210992221
Bytes recibidos/segundo: 675821,6888561849

```

Ejemplo: determinar durante cuánto tiempo han estado ejecutándose los procesos en segundo plano actuales y determinar su rendimiento efectivo en términos de tiempo y de archivos por segundo

Nota: La caducidad no informa acerca del número de bytes procesados.

```

select process_num as "Número",
process,
current_timestamp-start_time as "Tiempo transcurrido",
(cast(files_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Archivos/segundo",
(cast(bytes_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes/segundo"
from processes

```

```

Número: 1
PROCESS: Expiration
Tiempo transcurrido: 0 00:24:36,000000
Archivos/segundo: 6,3216755870092
Bytes/segundo: 0,00000000000000

```

Ejemplo: contar el número de nodos cliente que existen para cada tipo de plataforma

```

select platform_name,count(*) as "Número de nodos"
from nodes group by platform_name

```

PLATFORM_NAME	Número de nodos
AIX	6
SunOS	27
Win32	14
Linux	20

Ejemplo: contar el número de espacios de archivos que tiene cada nodo y obtener una lista de los nodos cliente por orden ascendente

```

select node_name, count(*) as "number of tablespaces"
from tablespaces group by node_name order by 2

```

NODE_NAME	número de espacios de archivos
-----	-----

ALBERT	2
MILTON	2
BARNEY	3
SEBASTIAN	3
MAILHOST	4
FALCON	4
WILBER	4
NEWTON	4
JEREMY	4
WATSON	5
RUSSELL	5

Ejemplo: obtener información estadística para calcular el número de volúmenes fuera del local cuyo espacio se reclama durante la reclamación de una agrupación de almacenamiento.

```
select * from summary where activity='OFFSITE RECLAMATION'

START_TIME: 2004-06-16 13:47:31.000000
END_TIME: 2004-06-16 13:47:34.000000
ACTIVITY: OFFSITE RECLAMATION
NUMBER: 4
ENTITY: COPYPOOL
COMMMETH:
ADDRESS:
SCHEDULE_NAME:
EXAMINED: 170
AFFECTED: 170
FAILED: 0
BYTES: 17821251
IDLE: 0
MEDIAP: 0
PROCESSES: 2
SUCCESSFUL: YES
VOLUME_NAME:
DRIVE_NAME:
LIBRARY_NAME:
LAST_USE:
COMM_WAIT:
NUM_OFFSITE_VOLS: 2
```

Ejemplo: identificar qué agrupaciones de almacenamiento contienen datos cuyos duplicados han eliminado los clientes

```
select stgpool_name,has_client_dedup_data from stgpools

STGPOOL_NAME          HAS_CLIENT_DEDUP_DATA
-----
ADPOOL                NO
ARCHIVEPOOL           NO
BACKUPPOOL            NO
COPYDEDUP             NO
COPYNODEDUP          NO
FILEPOOL              YES
FILEPOOL2             NO
LANFREEFILEPOOL      YES
SPACEMGPOOL          NO
```

Ejemplo: obtener información sobre la base de datos

```
select * from db

DATABASE_NAME: TSMDB1
TOT_FILE_SYSTEM_MB: 2048000
USED_DB_SPACE_MB: 12576
FREE_SPACE_MB: 1576871
TOTAL_PAGES: 983044
USABLE_PAGES: 982908
USED_PAGES: 977736
FREE_PAGES: 5172
BUFF_HIT_RATIO: 96.2
TOTAL_BUFF_REQ: 53967
SORT_OVERFLOW: 0
LOCK_ESCALATION: 0
```

```

PKG_HIT_RATIO: 70.0
LAST_REORG: 2010-07-15 17:32:55.000000
FULL_DEV_CLASS: OUTFILE
NUM_BACKUP_INCR: 0
LAST_BACKUP_DATE: 2010-01-21 10:37:59.000000
PHYSICAL_VOLUMES: 0
PAGE_SIZE:
NUM_BACKUP_STREAMS: 4

```

Ejemplo: obtener registros de detalle de estimaciones de PVU

Genere la estimación de PVU para un nodo denominado ACCTSRECSRV, que se utiliza en el producto IBM Spectrum Protect Extended Edition.

```
select * from pvuestimate_details where node_name='ACCTSRECSRV'
```

```

PRODUCT: PRODEE
LICENSE_NAME: MGSYSLAN
NODE_NAME: ACCTSRECSRV
LAST_USED: 2008-01-20 16:12:24.000000
TRYBUY: FALSE
PROC_VENDOR: IBM
PROC_BRAND: POWER5+ QCM
PROC_TYPE: 4
PROC_MODEL:
PROC_COUNT: 2
ROLE: SERVER
ROLE_OVERRIDE: USERREPORTED
ROLE_EFFECTIVE: SERVER
VALUE_UNITS: 50
VALUE_FROM_TABLE: YES
PVU: 100
SCAN_ERROR : NO
API_CLIENT: NO
PVU_AGNOSTIC: NO
HYPERVISOR: VMWARE
GUID: 01.2e.1c.80.e5.04-
      .11.da.aa.ab.00.-
      15.58.0b.d9.47
VERSION: 6
RELEASE: 3
LEVEL: 1
VENDOR_D: IBM(R)
BRAND_D: POWER5(TM) QCM
TYPE_D: Quad-core Module
MODEL_D: All Existing
PRODUCT_D: IBM Spectrum Protect Extended Edition

```

Descripciones de los campos

PRODUCT

Compilación de tipos de licencia en productos al nivel presentado en el mandato QUERY PVUESTIMATE. Los valores posibles son PRODEE, PROTBASIC, PRODDATARET, PRODMAIL, PRODDDB, PRODSYSB, PRODSFACE, PRODSAN, PRODERP o en blanco.

LICENSE_NAME

La licencia asignada a este nodo.

NODE_NAME

El nombre de nodo.

LAST_USED

Fecha y hora en que se conectó por última vez el nodo identificado al sistema bajo esta licencia.

TRYBUY

Indica si se ejecuta con la modalidad de prueba. Los valores posibles son TRUE o FALSE.

PROC_VENDOR

El nombre de proveedor de procesador que notifica el cliente.

PROC_BRAND

El nombre de marca de procesador que notifica el cliente.

PROC_TYPE

El tipo de procesador que notifica el cliente. Este valor refleja también el número de núcleos. Los valores de ejemplo son 1=SINGLE CORE, 2=DUO CORE y 4=QUAD CORE.

PROC_MODEL

El modelo de procesador que notifica el cliente.

PROC_COUNT

	La cantidad de procesador.
ROLE	El rol del nodo. Los valores posibles son CLIENT, SERVER u OTHER.
ROLE_OVERRIDE	Altera temporalmente el valor especificado en el mandato UPDATE NODE.
ROLE_EFFECTIVE	Rol real basado en los valores de los campos ROLE y ROLE_OVERRIDE.
VALUE_UNITS	La unidad de valor de procesador (PVU) asignada del procesador.
PVU	El valor de PVU calculado.
	$\text{PVU por nodo} = \text{número de procesadores por nodo} * \text{tipo de procesador} * \text{valor de pvu}$
	donde el tipo de procesador representa el número de núcleos y el valor de pvu es el valor definido para el tipo de procesador en la tabla de PVU de IBM®.
VALUE_FROM_TABLE	Distintivo que indica si la PVU se ha calculado basándose en la tabla de PVU de IBM. Los valores posibles son YES o NO. Si es NO, se aplica un valor 100 para cada nodo definido como un servidor. Si no hay ningún rol definido para un nodo, se utiliza el rol del servidor a efectos de cálculo de PVU.
SCAN_ERROR	Distintivo que indica si el cliente ha notificado información sobre licencias. Los valores posibles son YES o NO.
API_CLIENT	Distintivo que indica una aplicación de API. Los valores posibles son YES o NO.
PVU_AGNOSTIC	Distintivo que indica que el nivel de release de la versión del cliente es anterior a IBM Spectrum Protect V6.3. Si la versión es anterior a 6.3, no se esperan mediciones de PVU válidas. Los valores posibles son YES o NO.
HYPERVISOR	Nombre del software de máquina virtual que notifica el cliente.
GUID	Identificador exclusivo global (GUID) del sistema donde se ubica el nodo. El GUID se obtiene de la tabla de nodo.
VERSION	La versión del cliente.
RELEASE	El release del cliente.
LEVEL	El nivel del cliente.
VENDOR_D	Valor de visualización del proveedor del procesador de la tabla de PVU.
BRAND_D	Valor de visualización de la marca de procesador de la tabla de PVU.
TYPE_D	Valor de visualización del tipo de procesador de la tabla de PVU.
MODEL_D	Valor de visualización del modelo de procesador de la tabla de PVU.
PRODUCT_D	Valor de visualización del producto de la tabla de PVU. Son posibles los siguientes valores:
	<ul style="list-style-type: none"> • IBM Spectrum Protect • IBM Spectrum Protect Extended Edition • IBM Spectrum Protect para retención de datos • IBM Spectrum Protect for SAN • IBM Spectrum Protect for Space Management • IBM Spectrum Protect for Mail • IBM Spectrum Protect para bases de datos • IBM Spectrum Protect for Enterprise Resource Planning • IBM Spectrum Protect for System Backup and Recovery • Blanco

Ejemplo: obtener información de rol e información relacionada con PVU

En el ejemplo siguiente se muestran los resultados parciales de un nodo seleccionado, incluida la información de rol y la información relacionada con PVU. Los roles posibles son CLIENT, SERVER u OTHER. La PVU sólo se calcula para los nodos definidos como servidores.


```
select * from nodes
```

```
ROLE: CLIENT
  ROLE_O: USEREPORTED
  PVENDOR: INTEL
  PBRAND: INTEL
  PTYPE: 4
  PMODEL:
  PCOUNT: 1
HYPERVISOR:
  PAPI: NO
  SCANERROR: NO
```

Mandatos SET

Utilice los mandatos SET para especificar valores que afectan a varias operaciones de IBM Spectrum Protect.

- SET ACCOUNTING (activar o desactivar registros de contabilidad)
- SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)
- SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)
- SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)
- SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)
- SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)
- SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)
- SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)
- SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)
- SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)
- SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)
- SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)
- SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)
- SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)
- SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)
- SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)
- SET CONFIGMANAGER (Especificar un gestor de configuración)
- SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)
- SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)
- SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)
- SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)
- SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)
- SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)
- SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)
- SET DEPLOYPKGMR (Habilitar el gestor de paquetes de despliegue)
- SET DEPLOYREPOSITORY (Establece la vía de acceso de descarga para los paquetes de despliegue del cliente)
- SET DEPLOYMAXPKGS (Establecer el número máximo de paquetes de despliegue del cliente para almacenar)
- DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)
- SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)
- SET DRMCHECKLABEL (Especificar comprobación de etiquetas)
- SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener mandatos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)
- SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)
- SET DRMCOURIERNAME (Especificar el nombre del transportista)
- SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)
- SET DRMFILEPROCESS (Especificar el proceso de archivos)
- SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)
- SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)
- SET DRMPPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)
- SET DRMPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)
- SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)
- SET DRMRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)
- SET DRMVAULTNAME (Especificar el nombre de la cámara de seguridad)
- SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)
- SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)
- SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)



- SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)
- SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)
- SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)
- SET MAXCMDRETRIES (Establecer el número máximo de reintentos de mandato)
- SET MAXSCHEDULESESSIONS (Establecer número máximo de sesiones planificadas)
- SET MINPWLENGTH (Establecer longitud mínima de contraseña)
- SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)
- SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)
- SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)
- SET PASSEXP (Establecer fecha de caducidad de contraseña)
- SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)
- SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)
- SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)
- SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)
- SET REPLRETENTION (Establecer el período de retención de los registros de réplica)
- SET REPLSERVER (Establecer el servidor de réplica de destino)
- SET RETRYPERIOD (Establecer período de tiempo entre reintentos)
- SET SCHEDMODES (seleccionar modalidad de planificación central)
- SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)
- SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)
- SET SERVERNAME (Especificar el nombre del servidor)
- SET SERVERPASSWORD (Establecer contraseña de servidor)
- SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)
- SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)
- SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)
- SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)
- SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)
- SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)
- SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)
- SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)
- SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)
- SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)


SET ACCOUNTING (activar o desactivar registros de contabilidad)

Utilice este mandato para determinar si se crea un registro de contabilidad cada vez que finaliza una sesión de nodo cliente. Un registro de contabilidad realiza un seguimiento de la cantidad de almacenamiento que ha utilizado una sesión de nodo cliente.

Utilice el mandato QUERY STATUS para determinar si se han de generar registros de contabilidad. Durante la instalación, este valor se establece en OFF.

Los registros de contabilidad se guardan en un archivo de contabilidad llamado dsmacct.log.

 Sistemas operativos AIX  Sistemas operativos Linux La variable de entorno, DSMSERV_ACCOUNTING_DIR, especifica el directorio en el que se encuentra el archivo de contabilidad.

 Sistemas operativos Windows Una entrada de registro controla la ubicación del registro de contabilidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ACCounting---+ON---+-----<<
                '-OFF-'
```

Parámetros

ON

Especifica que el servidor crea un registro de contabilidad cada vez que finaliza una sesión de nodo cliente.

OFF

Especifica que el servidor no crea registros de contabilidad.

Ejemplo: crear registros de contabilidad

Para crear un registro de contabilidad al final de cada sesión de nodo cliente, emita el mandato siguiente:

```
set accounting on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ACCOUNTING

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)

Utilice este mandato para gestionar los registros de las anotaciones de actividad por fecha o tamaño. Las anotaciones de actividades contienen los mensajes de actividad normales que genera el servidor. Estos mensajes contienen información relativa a las operaciones del servidor y de los clientes, como por ejemplo, la hora de inicio de las sesiones o errores de E/S de dispositivos.

La información de las anotaciones de actividades incluye mensajes, como por ejemplo:

- La sesión cliente se inicia y finaliza
- La migración se inicia y finaliza
- Mensajes de error de diagnóstico
- Salida de mandatos de administración planificados

Durante la instalación del servidor, la gestión de las anotaciones de actividad está basada en la retención y el período de retención es de 30 días.

Puede ajustar el período de tiempo durante el que las anotaciones de actividad mantienen los mensajes para evitar datos insuficientes o caducados. El servidor elimina automáticamente los mensajes de las anotaciones de actividad una vez expirado el período de retención.

También puede optar por limitar el tamaño total de las anotaciones de actividad para controlar la cantidad de espacio que ocupan. El servidor eliminará periódicamente los registros de anotaciones de actividad más antiguos hasta que el tamaño de las anotaciones deje de superar el máximo permitido configurado.

Puede ejecutar el mandato QUERY STATUS para que se visualice el número actual de registros de las anotaciones de actividad y el tamaño (en megabytes) que ocupan actualmente las anotaciones de actividades.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ACTlogretention--número--+-Mgmtstyle-----Date-----+----->>
                                     '-Mgmtstyle-----+Date+-'
                                     '-Size-'
```

Parámetros

número (Obligatorio)

Especifica el número de días que se retienen los mensajes en las anotaciones de actividades cuando se gestionan por fecha, o especifica el tamaño máximo de las anotaciones de actividades cuando se gestionan por tamaño. En el caso de la gestión basada en la retención, un valor de 1 especifica que se han de retener los registros de las anotaciones de actividades durante el día de hoy. En el caso de la gestión basada en el tamaño, un valor de 1 especifica un tamaño máximo de 1 MB para las anotaciones. Puede especificar un número comprendido entre 0 y 9999. Un valor de 0 desactiva la retención de las anotaciones de actividades.

Mgmtstyle

Especifica si la gestión de las anotaciones de actividad se basa en la retención o el tamaño. Este parámetro es opcional. El valor predeterminado es DATE. Los valores posibles son:

Date

Especifica que la gestión de las anotaciones de actividad se basa en la retención.

Size

Especifica que la gestión de las anotaciones de actividad se basa en el tamaño.

Ejemplo: establecer el período de retención de las anotaciones de actividades

Establezca el servidor de modo que retenga los registros de anotaciones de actividades durante 60 días. Emita el mandato:

```
set actlogretention 60
```

Ejemplo: establecer el tamaño de las anotaciones de actividades

Establecer el servidor para que limite el tamaño de las anotaciones de actividad a 300 MB. Emita el mandato:

```
set actlogretention 300 mgmtstyle=size
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET ACTLOGRETENTION

Mandato	Descripción
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)

Utilice este mandato para especificar durante cuánto tiempo permanece activa una alerta antes de quedar inactiva. Si se desencadena de nuevo una alerta activa, se reinicia el tiempo de duración.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTACTiveduration -número_mins-----<<
```

Parámetros

número_mins (Necesario)

Especifica el número de minutos durante los cuales una alerta permanece activa antes de queda inactiva. Especifique un valor de 1 a 20160. El valor predeterminado inicial de servidor es 480 minutos.

Establecer la duración de una alerta activa a un día

Emita el siguiente mandato para especificar que las alertas permanezcan activas durante 1440 minutos antes de cambiar al estado inactivo:

```
set alertactiveduration 1440
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTACTIVEDURATION

Mandato	Descripción
---------	-------------

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)

Utilice este mandato para especificar durante cuánto tiempo permanece cerrada una alerta antes de que se suprima.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTCloseddurati on -número_mins-----><
```

Parámetros

número_mins (Necesario)

Especifica el número de minutos durante los cuales una alerta permanece cerrada antes de suprimirse. Si establece el valor en 0, las alertas se suprimen inmediatamente después de cerrarse. Especifique un valor de 0 a 99999. El valor predeterminado se establece en 60 minutos cuando se formatea inicialmente la base de datos de servidor de IBM Spectrum Protect.

Suprimir alertas dos horas después de que se hayan cerrado

Especifique que las alertas permanezcan cerradas durante 120 minutos antes de que se supriman:

```
set alertclosedduration 120
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTCLOSEDDURATION

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)

Utilice este mandato para permitir que las alertas se envíen por correo electrónico a los administradores especificados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTEMail---ON---+-----<
      '-OFF-'
```

Parámetros

ON

Especifica que las alertas se pueden enviar por correo electrónico a los administradores especificados.

OFF

Especifica que las alertas no se pueden enviar por correo electrónico a los administradores especificados. Cuando se formatea inicialmente la base de datos del servidor, el valor ALERTEMAIL se establece en OFF.

Habilitar alertas que se enviarán al administrador cuando se produzcan

Habilitar que se envíen las alertas por correo electrónico emitiendo el mandato siguiente:

```
SET ALERTEMAIL ON
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAIL

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)

Utilice este mandato para especificar la dirección de correo electrónico del remitente de la alerta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTEMAILFromaddr -dirección_correo_electrónico-----<
```

Parámetros

dirección_correo_electrónico (Necesario)

Especifica la dirección de correo electrónico del remitente. Las direcciones de correo electrónico tienen el formato de *nombre@dominio*. Los nombres de correo electrónico, incluida la dirección, no puede tener más de 64 caracteres de longitud y el nombre de dominio no puede tener más de 255 caracteres de longitud.

Especificar la dirección de correo electrónico del remitente de alerta

Especifique la dirección de correo electrónico del remitente emitiendo el mandato siguiente:

```
set alertemailfromaddr djadmin@mydomain.com
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILFROMADDR

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)

Utilice este mandato para especificar el nombre de host de servidor de correo de SMTP (Protocolo simple de transferencia de correo) que se utiliza para enviar el correo electrónico de alerta.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTEMAILSMTPHost--nombre_host-----<<
```

Parámetros

nombre_host (Necesario)

Especifica el nombre de host de servidor de correo SMTP.

Especifique el nombre de host del servidor de correo SMTP como mail.domain.com

Especifique `mail.domain.com` como el servidor de correo SMTP, emitiendo el siguiente mandato:

```
set alertemailsmtpghost mail.domain.com
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILSMTPHOST

Mandato	Descripción
---------	-------------

Mandato	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)

Utilice este mandato para especificar el número de puerto para el servidor de correo SMTP. Este servidor de correo se utiliza para enviar las alertas por correo electrónico.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTEMAILSMTPPort--puerto_tcp-----<<
```

Parámetros

puerto_tcp (Obligatorio)

Especifica el número de puerto del servidor de correo SMTP. Especifique un valor de 1 a 32767. El número de puerto predeterminado es 25.

Especificar el número de puerto del servidor de correo SMTP

Especifique el número de puerto 450 como servidor de correo SMTP emitiendo el siguiente mandato:

```
set alertemailsmtpport 450
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILSMTPPORT

Mandato	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)

Utilice este mandato para especificar los administradores que desean recibir resúmenes de alerta por correo electrónico, cada hora.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTSUMMARYToadmins---+nombre_admin+-----><
      ',-----'
```

Parámetros

nombre_admin (Necesario)

Especifica el nombre del administrador que desea recibir resúmenes de alerta por correo electrónico. Puede especificar un máximo de tres nombres de administrador separándolos con comas sin espacios intercalados.

Especificar dos administradores para que reciban resúmenes de alerta

Especifique que los administradores HARRY y COLIN desean recibir resúmenes de alertas, emitiendo el siguiente mandato:

```
set alertsummarytoadmins HARRY,COLIN
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTSUMMARYTOADMINS

Mandato	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.

SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)

Utilice este mandato para especificar durante cuánto tiempo permanece inactiva una alerta. Una vez que ha transcurrido el periodo de duración de inactividad, la alerta se cierra.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTINactiveduration -numero_mins-----><
```

Parámetros

número_mins (Necesario)

Especifica el número de minutos que una alerta permanece inactiva antes de que se cierre. Puede especificar un valor comprendido entre 1 – 20160. El valor predeterminado inicial de servidor es 480 minutos.

Cambiar el estado de alerta de inactivo a cerrado después de 60 minutos

Emita el siguiente mandato para especificar que una alerta permanezca en estado inactivo durante 60 minutos antes de cambiar al estado cerrado:

```
set alertinactiveduration 60
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTINACTIVEDURATION

Mandato	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)

Utilice este mandato para activar o desactivar el supervisor de alertas.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
..-OFF-.  
>>-Set ALERTMONITOR -+-ON-+-----<<
```

Parámetros

ON

Especifica que el servidor de IBM Spectrum Protect supervise las alertas.

OFF

Especifica que el servidor de IBM Spectrum Protect no supervise las alertas. Cuando se formatea inicialmente la base de datos de servidor de IBM Spectrum Protect, el valor de supervisión de alertas está establecido en OFF.

Activar la supervisión de alertas

Active la supervisión de alertas emitiendo el mandato siguiente:

```
set alertmonitor on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTMONITOR

Mandato	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.

Mandato	Descripción
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerra antes de suprimirse.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)

Utilice este mandato para especificar la frecuencia con la que el supervisor de alertas actualiza y borra las alertas que se almacenan en la base de datos de servidor de IBM Spectrum Protect.

Durante este intervalo de comprobación, el supervisor de alertas examina cada alerta en el servidor y realiza las acciones siguientes:

- El supervisor de alertas determina si han transcurrido los tiempos de duración de actividad o inactividad. Si transcurre el tiempo de duración especificada, el estado de alerta se actualiza al estado siguiente. Por ejemplo:
 - Activo a inactivo
 - Inactivo a cerrado
- En caso de que se cierre una alerta durante el tiempo especificado por el mandato SET ALERTCLOSEDDURATION, la alerta se suprime.

Puede utilizar el mandato QUERY MONITORSETTINGS para determinar si la supervisión de alertas está activa. Utilice el mandato SET ALERTMONITOR para activar la supervisión de alertas.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ALERTUPDateinterval -número_mins-----><
```

Parámetros

número_mins (Necesario)

Especifica el periodo de tiempo, en minutos, que el supervisor espera antes de que se actualicen y borren las alertas en el servidor. Especifique un valor de 1 a 9999. El servidor tiene un valor predeterminado inicial de 10 minutos.

Establecer intervalo de actualización de alertas en 60 minutos

Especifique que las alertas se actualicen cada hora emitiendo el mandato siguiente:

```
set alertupdateinterval 60
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ALERTUPDATEINTERVAL

Mandato	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerra antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.

SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)

Utilice este mandato para activar y desactivar la protección de retención de datos de copia archivada. Para que este mandato funcione, el servidor no debe contener datos. Durante la instalación este valor se establece en OFF.

Si la protección de retención de datos de copia archivada está activa:

- Sólo se pueden almacenar copias archivadas en el servidor.
- No se puede suprimir la copia archivada hasta que el parámetro RETVER en el mandato DEFINE COPYGROUP (archivo) esté satisfecho.

Sólo los servidores con protección de retención de datos habilitada soportan la definición de agrupaciones de almacenamiento del tipo RECLAMATIONTYPE=SNAPLOCK.

Utilice el mandato QUERY STATUS para que se visualice el estado de la protección de retención de datos de copia archivada.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-Set ARCHIVERETENTIONPROTECTION +-Off+-----<<  
      '-ON--'
```

Parámetros

- Off
Especifica que la protección de retención de datos de copia archivada no está activa.
- ON
Especifica que la protección de retención de datos de copia archivada sí está activa.

Ejemplo: activar la protección de retención de datos

Activar la protección de retención de datos de copia archivada con el mandato siguiente:

```
set archiveretentionprotection on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ARCHIVERETENTIONPROTECTION

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
AUDIT VOLUME	Compara la información de base de datos y de la agrupación de almacenamiento y, opcionalmente, resuelve las incoherencias.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

Mandato	Descripción
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)

Utilice este mandato para establecer la regla de réplica del servidor de los datos de archivado.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos de archivado se establecen en DEFAULT.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Puede especificar una regla de réplica de prioridad normal o una regla de réplica de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y prioridad alta, se replican primero los datos de prioridad alta. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos de archivado y datos de copia de seguridad. La réplica de los datos de archivado tiene una prioridad más alta que los datos de copia de seguridad. Para dar prioridad a los datos de archivado, emita el mandato SET ARREPLRULEDEFAULT y especifique la regla de réplica ALL_DATA_HIGH_PRIORITY. Para priorizar los datos de copia de seguridad, emita el mandato SET BKREPLRULEDEFAULT y especifique la regla de réplica ALL_DATA para los datos de copia de seguridad. La regla ALL_DATA para los datos de copia de seguridad replica los datos de copia de seguridad con una prioridad normal.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set ARREPLRuledefault---ALL_DATA-----+-----<<
      +-ALL_DATA_HIGH_PRIORITY--+
      '-NONE-----'
```

Parámetros

ALL_DATA
Hace una réplica de los datos de archivado con una prioridad normal.

ALL_DATA_HIGH_PRIORITY
Hace una réplica de los datos de archivado con una prioridad alta.

NONE
Los datos de archivado no se replican.

Ejemplo: establecer la regla de réplica del servidor para los datos de archivado

Configure la regla predeterminada para que los datos de archivado se repliquen con una prioridad alta.

```
set arreplruledefault all_data_high_priority
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET ARREPLRULEDEFAULT

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)

Utilice este mandato para establecer la regla de réplica del servidor de los datos de copia de seguridad.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos de copia de seguridad se establecen en DEFAULT.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a los datos de copia de seguridad, emita el mandato SET BKREPLRULEDEFAULT y especifique la regla de réplica ACTIVE_DATA_HIGH_PRIORITY. Para priorizar los datos de archivado, emita el mandato SET ARREPLRULEDEFAULT y especifique la regla de réplica ALL_DATA para los datos de archivado. La regla ALL_DATA para los datos de archivado replica los datos de archivado con una prioridad normal.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set BKREPLRuledefault---ALL_DATA-----+-----<<
      +-ACTIVE_DATA-----+
      +-ALL_DATA_HIGH_PRIORITY----+
      +-ACTIVE_DATA_HIGH_PRIORITY--+
      '-NONE-----'
```

Parámetros

ALL_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro FORCERECONCILE=YES.

- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL_DATA_HIGH_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE_DATA excepto que los datos se replican con una prioridad alta.

NONE

Los datos de copia de seguridad no se replican.

Ejemplo: establecer la regla de réplica del servidor para los datos de copia de seguridad

Configure la regla predeterminada para que los datos de seguridad repliquen solo los datos activos y para que se repliquen los datos con una prioridad alta.

```
set bkreplruledefault active_data_high_priority
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET BKREPLRULEDEFAULT

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET REPLRETENTION	Especifica el periodo de retención de los registros de historial de réplicas.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)

Utilice este mandato para especificar la duración de la planificación que se ha definido con el mandato DEFINE CLIENTACTION. Una acción del cliente define una planificación que se ejecuta una vez en un cliente.

El programa suprime estos registros de eventos independientemente de si el cliente ha procesado la planificación. Sin embargo, estas planificaciones no se suprimen hasta que se suprime el primer registro de eventos. El período de retención de eventos se establece de forma predeterminada en 10 días a partir de la instalación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET CLIENTACTDuration--días-----<<
```

Parámetros

días (Obligatorio)

Especifica el número de días durante el cual estará activa la planificación de la acción del cliente. Puede especificar un entero de 0 a 999. El valor predeterminado son 5 días.

El número de días que especifique determina durante cuánto tiempo la base de datos retiene la planificación antes de suprimirla. El valor 0 indica que la duración de la planificación es indefinida y que la planificación y las asociaciones no se suprimen de la base de datos.

Ejemplo: establecer un período de duración de 15 días para la acción del cliente.

Para especificar que la planificación de la acción del cliente esté activa durante 15 días, emita el mandato siguiente:

```
set clientactduration 15
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET CLIENTACTDURATION

Mandato	Descripción
DEFINE CLIENTACTION	Define un mandato que se ha de realizar en un nodo cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET CONFIGMANAGER (Especificar un gestor de configuración)

Utilice este mandato para especificar si un servidor es un gestor de configuración. En un gestor de configuración, puede definir perfiles de configuración a los que otros servidores pueden suscribirse.

No se puede designar un servidor como gestor de configuración si el servidor se suscribe a uno o más perfiles de otro gestor de configuración.

Si un servidor es un gestor de configuración, no puede cambiar esta designación hasta que suprima todos los perfiles, incluyendo el perfil predeterminado.

Emita el mandato QUERY STATUS para determinar si un servidor es un gestor de configuración. Cuando se instala un servidor, no se designa como gestor de configuración.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set CONFIGManager--+-OFF-+-----<<
                        '-ON--'
```

Parámetros

ON

Especifica que el servidor es un gestor de configuración.

Al designar un servidor como gestor de configuración, IBM Spectrum Protect crea un perfil predeterminado denominado DEFAULT_PROFILE y asocia al perfil todos los servidores y grupos de servidores definidos en el gestor de configuración. Puede modificar o suprimir el perfil predeterminado.

OFF

Especifica que el servidor no es un gestor de configuración.

Ejemplo: especificar un gestor de configuración

Designar un servidor como gestor de configuración.

```
set configmanager on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET CONFIGMANAGER

Mandato	Descripción
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET CONFIGREFRESH	Especifica un intervalo de tiempo para que los servidores gestionados entren en contacto con los gestores de configuración.

SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)

Utilice este mandato en un servidor gestionado para especificar la frecuencia con la que ese servidor establece contacto con su gestor de configuración para obtener información de configuración actualizada.

Para que se visualice el valor actual, emita el mandato QUERY STATUS. En la instalación, el intervalo se establece en 60 minutos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set CONFIGRefresh--minutos-----<<
```

Parámetros

minutos (Obligatorio)

Especifica el intervalo, en minutos, antes de que un servidor gestionado se ponga en contacto con su servidor de configuración para obtener las actualizaciones de configuración. Especifique un entero de 0 a 10000.

- Si el valor es mayor que 0, el servidor gestionado establece contacto con el gestor de configuración inmediatamente. El siguiente contacto se produce al alcanzar el intervalo especificar.
- Si el valor es 0, el servidor gestionado no establece contacto con el gestor de configuración.

Se prescinde de este valor si el servidor no se inscribe como mínimo en un perfil de un gestor de configuración.

Ejemplo: establecer un intervalo de renovación de 45 minutos

Especificar que un servidor gestionado contacte con su gestor de configuración cada 45 minutos.

```
set configrefresh 45
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET CONFIGREFRESH

Mandato	Descripción
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UPDATE PROFILE	Cambia la descripción de un perfil.

SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)

Utilice este mandato para obtener información adicional cuando aparezcan mensajes ANR9999D. IBM Spectrum Protect sondea los componentes del servidor en busca de información como el nombre de proceso, el nombre de la hebra, el identificador de sesión, los datos de transacción, los bloqueos mantenidos y las tablas de base de datos que se están utilizando.

Nota: Cuando un subproceso emite mensajes consecutivos de la misma área de código, sólo el primer mensaje proporciona información de contexto.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set CONTEXTmessaging--+-ON--+-----<<
      '-OFF-'
```

Parámetros

- ON
Especifica que se activa el informe de contexto de mensajes.
- OFF
Especifica que se desactiva el informe de contexto de mensajes.

Ejemplo: activar o desactivar el informe de contexto de mensajes

Activar el envío de mensajes de contexto para recibir información adicional que puede ayudar a determinar la causa de los mensajes ANR9999D.

```
set contextmessaging on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET CONTEXTMESSAGING

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)

Utilice este mandato para especificar el número de días entre exploraciones de cliente de la información de estación de trabajo que se utiliza para calcular la unidad de valor de procesador (PVU).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set CPUINFOREFRESH--días-----<<
```

Parámetros

días (Obligatorio)

Especifica el número de días entre exploraciones de dispositivos de cliente. Para recuperar el valor actual, emita el mandato QUERY STATUS. Los valores posibles son de 1 a 9999. El valor predeterminado es 180.

Ejemplo: Establecer la cantidad de tiempo antes de la siguiente renovación en 90 días

```
SET CPUINFOREFRESH 90
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET CPUINFOREFRESH

Mandato	Descripción
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.

SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)

Utilice este mandato para especificar si un servidor se define automáticamente en otro servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set CROSSDefine--+-ON--+-----<<  
                  '-Off-'
```

Parámetros

ON

Especifica que un servidor se puede definir en otro servidor. Para definir automáticamente un servidor en otro, también debe permitir la definición cruzada de un servidor en la definición del otro servidor.

OFF

Especifica que un servidor no se puede definir en otro servidor.

Ejemplo: especificar si los servidores se definen el uno en el otro

Establecer una definición cruzada que permita que la definición de un servidor esté en otro servidor.

```
set crossdefine on
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET CROSSDEFINE

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.

SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)

Utilice este mandato para especificar la clase de dispositivo y el número de corrientes de datos que se utilizarán para las copias de seguridad de base de datos automáticas. También puede utilizar este mandato para configurar el mandato BACKUP DB para hacer copia de seguridad automáticamente de la clave de cifrado maestra para el servidor.

La clave de cifrado maestra se utiliza para cifrar datos en agrupaciones de almacenamiento de contenedor en el directorio y de contenedor en la nube, y para cifrar información confidencial en la base de datos del servidor. Si no hace copia de seguridad de la clave de cifrado maestra, es posible que no pueda acceder a ninguno de esos elementos cifrados si se produce un desastre.

Si ejecuta el mandato BACKUP DB y la clase de dispositivo no es la especificada en el mandato SET DBRECOVERY, se devuelve un mensaje de aviso. Sin embargo, la operación de copia de seguridad continuará y no se verá afectada por ello.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

```
>>-SET DBRECOVery--nombre_clase_dispositivo----->
      .-NUMStreams---1----- .-COMPRESS---No-----
>+-----+-----+-----+-----+-----+----->
      '-NUMStreams---número-' '-COMPRESS---No--+'
                                     '-Yes-'

      .-PROTECTKeys---Yes-----
>+-----+-----+-----+-----+-----+----->
      '-PROTECTKeys---No--+'
                                     '-Yes-'

>+-----+-----+-----+-----+-----+-----><
      '-PASSWORD---nombre_contraseña-'
```

Parámetros

nombre_clase_dispositivo (**Necesario**)

Especifica la clase de dispositivo que debe utilizarse para las copias de seguridad de bases de datos.

NUMStreams

Especifica el número de corrientes de movimiento de datos paralelas que se utilizan cuando se realiza la copia de seguridad de la base de datos. El valor predeterminado mínimo es de 1 y el valor máximo es de 32. Si se aumenta este valor se produce un aumento correspondiente en el número de sesiones de copia de seguridad de base de datos que se han de utilizar y en el número de unidades que se han de utilizar para la clase de dispositivo. Si se especifica un valor NUMSTREAMS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. El valor NUMSTREAMS se utiliza para todos los tipos de copias de seguridad de base de datos.

Si se especifica un valor mayor que el número de unidades disponibles para la clase de dispositivo, se utiliza el número de unidades disponibles. Las unidades disponibles son las definidas en la clase de dispositivo por el parámetro MOUNTLIMIT o por el número de unidades en línea para la clase de dispositivo especificada. La sesión se visualiza en la salida de QUERY SESSION. Si aumenta el número de corrientes, se utilizan más volúmenes de la clase de dispositivo correspondiente a esta operación. El uso de más volúmenes puede mejorar la velocidad de las copias de seguridad de base de datos, pero a expensas de que haya más volúmenes que no se utilizan completamente.

COMPRESS

Especifica si se comprimen los volúmenes durante el proceso de copia de seguridad de bases de datos. Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los valores siguientes:

No

Especifica que los volúmenes que se crean mediante el mandato BACKUP DB no se comprimen.

Yes

Especifica que los volúmenes que se crean mediante el mandato BACKUP DB se comprimen.

Si especifica el parámetro COMPRESS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. De lo contrario, se utiliza el valor establecido en el mandato SET DBRECOVERY.

Restricciones:

- Tenga cuidado al especificar el parámetro COMPRESS. La utilización de compresión durante las copias de seguridad de la base de datos puede reducir el tamaño de los archivos de copia de seguridad. Sin embargo, la compresión puede aumentar el tiempo necesario para completar el proceso de copia de seguridad de base de datos.
- No realice copias de seguridad de datos comprimidos en una cinta. Si el entorno del sistema almacena copias de seguridad de bases de datos en la cinta, establezca el parámetro COMPRESS en No en los mandatos SET DBRECOVERY y BACKUP DB.

PROTECTKeys

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es Yes (sí).

Puede especificar uno de los valores siguientes:

No

Especifica que las copias de seguridad de base de datos no incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=NO, debe hacer copia de seguridad de la clave de cifrado maestra manualmente para el servidor y hacer que la clave está disponible cuando implementa la recuperación tras desastre.

Yes

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=YES, también debe especificar el parámetro PASSWORD.

PASSword

Especifica la contraseña que se utiliza para proteger las copias de seguridad de base de datos. El valor predeterminado es proteger las copias de seguridad de base de datos.

Importante: Asegúrese de que recuerda esta contraseña. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos.

Ejemplo: especificar una clase de dispositivo para copias de seguridad de bases de datos

Especificar la clase de dispositivo DBBACK para copias de seguridad de bases de datos. Ejecute el mandato siguiente:

```
set dbrecovery dbback
```

Ejemplo: especificar una clase de dispositivo y el número de corrientes para copias de seguridad de bases de datos

Especifique la clase de dispositivo DBBACK para las copias de seguridad de bases de datos y especifique que la copia de seguridad utilice dos corrientes de movimiento de datos. Ejecute el mandato siguiente:

```
set dbrecovery dbback numstreams=2
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: Proteger las claves de cifrado de la agrupación de almacenamiento en copias de seguridad de base de datos

Cifrar los datos de agrupación de almacenamiento especificando que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Ejecute el mandato siguiente:

```
set dbrecovery dbback protectkeys=yes password=password_name
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DBRECOVERY

Mandato	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)

Utilice este mandato para verificar las extensiones enviadas al servidor durante la eliminación de datos duplicados del lado del cliente.

Una aplicación invasora que reside en un sistema cliente y que imita al cliente, la API o la GUI y puede iniciar un ataque en el servidor. Para proteger al servidor a tales ataques, puede especificar un porcentaje de extensiones de cliente para que las verifique el servidor.

Si el servidor detecta que hay un ataque de seguridad en curso, se cancela la sesión actual. Además se cambia el valor del parámetro DEDUPLICATION del mandato REGISTER NODE. El valor cambia de CLIENTORSERVER a SERVERONLY. El valor SERVERONLY inhabilita la eliminación de datos duplicados del lado del cliente en ese nodo.

El servidor también emite un mensaje avisando de que se ha detectado un ataque potencial contra la seguridad y que la eliminación de datos duplicados del lado del cliente se ha inhabilitado en ese nodo. Si se inhabilita la eliminación de datos duplicados del lado del cliente, todas las demás operaciones del cliente (por ejemplo, las operaciones de copia de seguridad) continúan. Sólo se inhabilita la eliminación de datos duplicados del lado del cliente. Si se inhabilita la eliminación de datos duplicados del lado del cliente en un nodo porque se ha detectado un ataque potencial, el servidor elimina los duplicados de los datos elegibles para la eliminación de datos duplicados del lado del cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DEDUPVERificationlevel--+-0-----+-----><
                               '-valor_porcentaje-'
```

Parámetros

valor_porcentaje (Obligatorio)

Especifique un valor entero entre 0 y 100 para indicar el porcentaje de extensiones del cliente que se deben verificar. El valor 0 indica que no se verifica ninguna extensión del cliente. El valor predeterminado para este mandato es 0.

Consejos:

- La verificación de extensiones consume potencia de procesamiento y perjudica el rendimiento del servidor. Para obtener un rendimiento óptimo, no especifique valores superiores a 10 en este mandato.
- Para visualizar el valor actual de SET DEDUPVERIFICATIONLEVEL, emita el mandato QUERY STATUS.

Ejemplo: especificar un nivel mínimo de verificación de eliminación de datos duplicados

Para especificar que se verifique el 1% de las extensiones creadas durante la eliminación de datos duplicados del lado del cliente, emita el siguiente mandato:

```
set dedupverificationlevel 1
```

Ejemplo: desactivar la verificación de la eliminación de datos duplicados

Para especificar que no se verifique ninguna de las extensiones creadas durante la eliminación de datos duplicados del lado del cliente, emita el siguiente mandato:

```
set dedupverificationlevel 0
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DEDUPVERIFICATIONLEVEL

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)

Utilice este mandato para configurar el método de autenticación de contraseña predeterminada para nodos y administradores que son resultado de los mandatos REGISTER NODE o REGISTER ADMIN .

Si especifica LDAP, establece el valor predeterminado para autenticarse en un directorio externo para cualquier mandato REGISTER NODE o REGISTER ADMIN nuevo. Este mandato facilita el registro de los nodos o administradores cuando se utiliza un servidor de directorios LDAP.

Consejo: El valor de autenticación predeterminado se puede sobrescribir cuando se especifica el método de autenticación en un REGISTER NODE o REGISTER ADMIN.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET DEFAULTAUTHentication---Local-----<<  
      '-LDap--'
```

Parámetros

Local

Especifica que cualquier mandato REGISTER NODE o REGISTER ADMIN que emita en el futuro utilizará LOCAL como valor del parámetro de autenticación predeterminado. Las contraseñas autenticadas localmente son las que se almacenan en el servidor de IBM Spectrum Protect. Las contraseñas autenticadas a nivel local no distinguen entre mayúsculas y minúsculas.

LDap

Especifica que cualquier mandato REGISTER NODE o REGISTER ADMIN que emita en el futuro utilizará LDAP como valor del parámetro de autenticación predeterminado. Las contraseñas autenticadas mediante LDAP son aquellas que se almacenan en el servidor de directorios LDAP y distinguen entre mayúsculas y minúsculas.

Ejemplo: establecer el valor de autenticación de contraseña predeterminada en LDAP

Especifique que cualquier mandato REGISTER NODE o REGISTER ADMIN que emite autentica contraseñas con un servidor de directorios LDAP.

```
set defaultauthentication ldap
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DEFAULTAUTHENTICATION

Mandato	Descripción
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.

SET DEPLOYPKGMR (Habilitar el gestor de paquetes de despliegue)

Utilice este mandato para habilitar o inhabilitar el gestor de paquetes de despliegue. Este componente descarga los paquetes de despliegue del cliente desde el sitio FTP para la instalación automática mediante el Centro de operaciones.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

                .-ON--.
>>-SET DEPLOYPKGMr---OFF-+-----><

```

Parámetros

ON

Especifica que el gestor de paquetes de despliegue consulta el sitio FTP para obtener nuevos paquetes de despliegue y los descarga cuando están disponibles. Este es el valor predeterminado.

OFF

Especifica que el gestor de paquetes de despliegue no consulta el sitio FTP ni descarga nuevos paquetes. Si inhabilita el gestor de paquetes de despliegue mientras se están descargando paquetes, los procesos de descarga activos continuarán ejecutándose hasta que se completen.

Ejemplo: Inhabilitar el gestor de paquetes de despliegue

Inhabilite el gestor de paquetes de despliegue emitiendo el mandato siguiente:

```
set deploypkgmgr off
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DEPLOYPKGMR

Mandato	Descripción
QUERY MONITORSETTINGS	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET DEPLOYREPOSITORY	Especifica la ubicación donde se descargan los paquetes de despliegue del cliente.

SET DEPLOYREPOSITORY (Establece la vía de acceso de descarga para los paquetes de despliegue del cliente)

Utilice este mandato para especificar la ubicación donde el proceso de despliegue automático descarga el despliegue más reciente de paquetes de cliente. Los paquetes de despliegue se utilizan para instalar actualizaciones en los sistemas cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET DEPLOYREpository--nombre_vía_acceso-----<
```

Parámetros

nombre_vía_acceso (Obligatorio)

Especifica la vía de acceso completa donde se descargan los paquetes de despliegue. Esta vía de acceso también especifica la ubicación donde el servidor coloca los archivos que representan los volúmenes de almacenamiento para la clase de dispositivo del despliegue de cliente. Puede eliminar vías de acceso emitiendo el mandato sin especificar un valor o especificando un valor vacío (""). Si no especifica un nombre de vía de acceso, el servidor no descargará paquetes de despliegue.

Cuando modifique la ubicación donde se almacenan los paquetes de actualización, los paquetes descargados anteriormente se suprimen automáticamente. Los volúmenes del servidor se suprimen a medida que los datos se recortan o caducan.

Importante: No suprima manualmente los archivos que tengan una extensión de nombre de archivo de .BFS. Los archivos BFS son volúmenes gestionados por el servidor, y contienen datos de archivado que caducan o se recortan automáticamente.

Ejemplo: especificar un nombre de vía de acceso

Especificar `/source/packages/` como la ubicación donde descargar los paquetes de despliegue. La misma ubicación se utiliza para la clase de dispositivo `IBM_DEPLOY_CLIENT_IMPORT`, que se utiliza para el despliegue del cliente.

```
set deployrepository /source/packages/
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DEPLOYREPOSITORY

Mandato	Descripción
QUERY MONITORSETTINGS	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET DEPLOYMAXPKGS	Especifica el número máximo de paquetes de despliegue de cliente que se descargarán y almacenarán en el servidor.

SET DEPLOYMAXPKGS (Establecer el número máximo de paquetes de despliegue del cliente para almacenar)

Utilice este mandato para especificar el número máximo de paquetes de despliegue del cliente instalables que se han descargado y almacenado en el servidor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET DEPLOYMAXPkgs--número-----<
```

Parámetros

número

Especifica el número máximo de paquetes de despliegue que se almacenan en el repositorio de despliegue para cada versión del producto. El número mínimo de paquetes es 1, y el número máximo es 4. Si se reduce el número, las versiones anteriores se

eliminarán la próxima vez que se renueven los paquetes. Los paquetes pueden tardar hasta un día en renovarse. El valor predeterminado es 4.

Ejemplo: Especificar el número máximo de paquetes de despliegue

Especifica 3 como número máximo de paquetes de despliegue que se descargan y almacenan.

```
set deploymaxpkgs 3
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DEPLOYMAXPKGS

Mandato	Descripción
QUERY MONITORSETTINGS	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET DEPLOYREPOSITORY (Establece la vía de acceso de descarga para los paquetes de despliegue del cliente)	Especifica la ubicación donde se descargan los paquetes de despliegue del cliente.

DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)

Utilice el mandato SET DISSIMILARPOLICIES para habilitar las políticas que están definidas en el servidor de réplica de destino para gestionar datos del nodo cliente replicados. Si no utiliza las políticas en el servidor de réplica de destino, los datos del nodo cliente replicados se gestionan mediante políticas en el servidor de réplica de origen.

Asegúrese de que esté instalado IBM Spectrum Protect versión 7.1.1 o posterior en los servidores de réplica de origen y destino antes de emitir este mandato. Emita este mandato en el servidor de réplica de origen.

Antes de utilizar las políticas que están definidas en un servidor de réplica de destino, debe emitir el mandato VALIDATE REPLPOLICY para ese servidor de réplica de destino. Este mandato muestra las diferencias entre las políticas para los nodos cliente en el servidor de réplica de origen y las políticas en el servidor de réplica de destino. Puede modificar las políticas en el servidor de réplica de destino antes de habilitar estas políticas para gestionar datos de nodo cliente replicados.

Para obtener el nombre del servidor de réplica de destino para el que desea gestionar datos y para comprobar si las políticas en el servidor de réplica de destino se establecen en ON, utilice el mandato QUERY REPLSERVER. Durante la instalación este valor se establece en OFF.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DISSIMILARPolicies--nombre_servidor_destino--+-+-----+-----><
                                     .-OFF-.
                                     +-OFF-+
                                     '-ON--'
```

Parámetros

nombre_servidor_destino (Obligatorio)

Especifica el nombre del servidor de réplica de destino para el que desea habilitar las políticas.

ON

Especifica que los datos del nodo cliente replicados los gestionan políticas que están definidas en el servidor de réplica de destino.

Off

Especifica que los datos del nodo cliente replicados los gestionan políticas que están definidas en el servidor de réplica de origen. El valor predeterminado es desactivado (Off).

Ejemplo: utilice las políticas en un servidor de réplica de destino

Para datos de nodo cliente replicados del servidor de réplica de destino, CVTCVS_LXS_SRV2, emita el mandato siguiente en el servidor de réplica de origen:

```
set dissimilarpolicies CVTCVS_LXS_SRV2 on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con DISSIMILARPOLICIES SET

Mandato	Descripción
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
VALIDATE REPLPOLICY	Verifica las políticas en el servidor de réplica de destino.

SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)

Utilice este mandato para especificar los nombres de las agrupaciones de datos activos que han de recuperarse tras haberse producido un siniestro. IBM Spectrum Protect utiliza estos nombres si el mandato PREPARE , MOVE DRMEDIA o QUERY DRMEDIA no incluye el parámetro ACTIVEDATASTGPOOL.

De manera predeterminada, los volúmenes de las agrupaciones de datos activos no pueden seleccionarse para que el gestor de recuperación ante siniestro los procese. Para procesar volúmenes de agrupación de datos activos, debe emitir el mandato SET DRMACTIVEDATASTGPOOL o debe utilizar el parámetro de línea de mandatos ACTIVEDATASTGPOOL en el mandato MOVE DRMEDIA, QUERY DRMEDIA o PREPARE.

Utilice el mandato QUERY DRMSTATUS para que se visualicen los valores actuales.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMACTIVEDatastgpool----->
      .-,-----
      v                                     |
>----nombre_agrupación_datos_activos-+-----<<
```

Parámetros

nombre_agrupación_datos_activos (Necesario)

Especifica los nombres de agrupación de datos activos. Cuando existan varios nombres, separe éstos mediante comas, sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados alterarán temporalmente los valores anteriores. Si especifica una serie nula (""), se eliminarán todos los nombres actuales y no se procesará ningún volumen de agrupación de datos activos cuyo estado sea MOUNTABLE si no se han especificado explícitamente como parámetros del mandato MOVE DRMEDIA, QUERY DRMEDIA o PREPARE.

Ejemplo: establecer una agrupación de datos activos como agrupación que puede seleccionarse

Establecer ACTIVEDATAPOOL1 como agrupación de datos activos que puede seleccionarse.

```
set drmactivedatapool activedatastgpool1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMACTIVEDATASTGPOOL

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.

Mandato	Descripción
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.

SET DRMCHECKLABEL (Especificar comprobación de etiquetas)

Utilice este mandato para especificar si IBM Spectrum Protect ha de leer las etiquetas de los medios secuenciales a los que se ha dado de baja mediante el mandato MOVE DRMEDIA. En la instalación, el valor de DRMCHECKLABEL se establece en YES.

Utilice el mandato QUERY DRMSTATUS para comprobar los valores actuales.

 Sistemas operativos AIX  Sistemas operativos Linux Este mandato no se utiliza con los tipos de dispositivo 349X.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMCHECKLabel--+-+-----+----->>
                    .-Yes-.
                    +-Yes-+
                    '-No--'
```

Parámetros

Yes

Especifica que IBM Spectrum Protect ha de leer las etiquetas de los medios secuenciales a los que se ha dado de baja mediante el mandato MOVE DRMEDIA.

No

Especifica que IBM Spectrum Protect no lee las etiquetas de los medios secuenciales que ha dado de baja el mandato MOVE DRMEDIA.

Ejemplo: Especificar que no se realice la comprobación de etiquetas

Especifique que no se realizado ninguna comprobación de etiquetas.

```
set drmchecklabel no
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMCHECKLABEL

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener mandatos)

Utilice este mandato para especificar el nombre del archivo que puede contener los mandatos que se crean al emitir los mandatos MOVE DRMEDIA o QUERY DRMEDIA. Si no se emite SET DRMCMDFILENAME, los mandatos MOVE DRMEDIA o QUERY DRMEDIA generan un nombre de archivo.

Utilice el mandato QUERY DRMSTATUS para que se muestre el nombre de archivo de mandatos actual.

Clase de privilegio

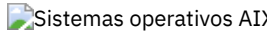
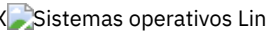
Para emitir este mandato, debe tener privilegio de sistema.

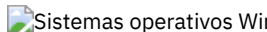
Sintaxis

```
>>-Set DRMCMDfilename--nombre_archivo-----><
```

Parámetros

nombre_archivo (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el nombre de la ruta completa del archivo que ha de contener los mandatos que se han creado mediante los mandatos MOVE DRMEDIA o QUERY DRMEDIA.

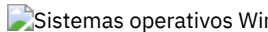
 Sistemas operativos Windows Especifica el nombre de la ruta completa del archivo que ha de contener los mandatos que se han creado mediante los mandatos MOVE DRMEDIA o QUERY DRMEDIA. El nombre del archivo puede contener un máximo de 259 caracteres.

Atención: Si ya existe un archivo con el mismo nombre, los mandatos MOVE DRMEDIA o QUERY DRMEDIA intentan utilizarlo, y se graba encima de los datos existentes.

Ejemplo: especificar el nombre del archivo que ha de contener los mandatos DRMEDIA

 Sistemas operativos AIX  Sistemas operativos Linux Especificar el nombre de archivo /adsm/drm/orm/exec.cmds.

```
set drmcmdfilename /adsm/drm/orm/exec.cmds
```

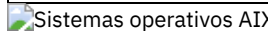
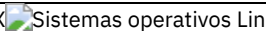
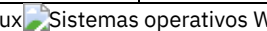
 Sistemas operativos Windows Especificar el nombre de archivo c:\drm\orm\exec.cmd.

```
set drmcmdfilename c:\drm\orm\exec.cmd
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMCMDFILENAME

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)

Utilice este mandato para especificar las agrupaciones de almacenamiento de copia de contenedor que ha de procesar el mandato MOVE DRMEDIA o QUERY DRMEDIA cuando ese mandato no incluye el parámetro COPYCONTAINERSTGPOOL.

De forma predeterminada, los mandatos MOVE DRMEDIA y QUERY DRMEDIA no procesan los volúmenes de las agrupaciones de almacenamiento de copia de contenedor. Debe emitir el mandato SET DRMCOPYCONTAINERSTGPOOL o utilizar el parámetro COPYCONTAINERSTGPOOL en el mandato MOVE DRMEDIA o QUERY DRMEDIA.

Consejo: Para visualizar los valores actuales, utilice el mandato QUERY DRMSTATUS.

Clase de privilegio

Para emitir este mandato, debe tener privilegios del sistema.

Sintaxis

```
      .-,-----  
      v |  
>>-Set DRMCOPYContainerstgpool----nombre_agrupación+-----><
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica los nombres de las agrupaciones de almacenamiento de copia de contenedor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados sustituyen a todos los valores anteriores. Si especifica una serie nula (""), se eliminan todos los nombres actuales.

Ejemplo: especifique las agrupaciones de almacenamiento que han de procesar los mandatos MOVE DRMEDIA y QUERY DRMEDIA

Establezca CONTCOPY1 y CONTCOPY2 como las agrupaciones de almacenamiento de copia de contenedor a procesar.

```
set drmcopycontainerstgpool contcopy1,contcopy2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMCOPYCONTAINERSTGPOOL

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)

Utilice este mandato para especificar los nombres de las agrupaciones de almacenamiento de copia que se recuperarán a continuación de un siniestro. IBM Spectrum Protect utiliza estos nombres si el mandato PREPARE no incluye el parámetro COPYSTGPOOL.

Si el mandato MOVE DRMEDIA o QUERY DRMEDIA no incluye el parámetro COPYSTGPOOL, el mandato procesa los volúmenes cuyo estado es MOUNTABLE y que se encuentran en la agrupación de almacenamiento de copia que indica el mandato SET DRMCOPYSTGPOOL. En la instalación, todas las agrupaciones de almacenamiento de copia se pueden seleccionar para el proceso de DRM.

Utilice el mandato QUERY DRMSTATUS para que se visualicen los valores actuales.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
      .-,-----  
      v |  
>>-Set DRMCOPYstgpool----nombre_agrupación_copia+-----><
```

Parámetros

nombre_agrupación_copia (Obligatorio)

Especifica los nombres de agrupación de almacenamiento de copia. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados sustituyen a todos los valores anteriores. Si

especifica una serie nula (""), se eliminan todos los nombres actuales y se pueden seleccionar todas las agrupaciones de almacenamiento de copia para el proceso.

Ejemplo: establecer una agrupación de almacenamiento de copia como agrupación que puede seleccionarse

Establecer COPYSTGPOOL1 como la agrupación de almacenamiento de copia seleccionable.

```
set drmcopystgpool copystgpool1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMCOPYSTGPOOL

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.

SET DRMCOURIERNAME (Especificar el nombre del transportista)

Utilice este mandato para especificar el nombre del transportista. En la instalación, este nombre se establece en COURIER. El mandato MOVE DRMEDIA utiliza el nombre del transportista para establecer la ubicación de los volúmenes que se establecen en el estado COURIER.

Puede utilizar QUERY DRMSTATUS para ver el nombre del transportista.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMCOURiername--courier_name-----><
```

Parámetros

nombre_transportista (Obligatorio)

Especifica el nombre del transportista. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

Ejemplo: establecer el nombre del transportista

Establecer el nombre del transportista en Joe's Courier Service.

```
set drmcouriername "Joe's Courier Service"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMCOURIERNAME

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.

Mandato	Descripción
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

Utilice este mandato para especificar cuándo una serie de copia de seguridad de base de datos es seleccionable para caducarla.

El valor que establece este mandato se aplica tanto a una serie de copia de seguridad de instantánea de base de datos como a una serie de copia de seguridad de base de datos completa e incremental. Cualquier tipo de serie de copia de seguridad de base de datos se considera seleccionable para caducidad si se cumplen todas las condiciones siguientes:

- La antigüedad del último volumen de la serie supera el valor de caducidad establece con el mandato SET DRMDBBACKUPEXPIREDAYS y el valor especificado para el parámetro DELgraceperiod con el mandato DEFINE SERVER. El parámetro DELgraceperiod solo se aplica a las copias de seguridad de base de datos remotas. El valor predeterminado para el parámetro DELgraceperiod es de 5 días. Por ejemplo, si establece el valor para el mandato SET DRMDBBACKUPEXPIREDAYS en 7 días y establece el valor para el parámetro DELgraceperiod en 6 días, la serie de copia de seguridad de base de datos remota no caduca hasta que han transcurrido 13 días.
- En el caso de los volúmenes que no son volúmenes virtuales, todos los volúmenes de la serie se encuentran en el estado VAULT.
- El volumen no forma parte de la serie de copia de seguridad de base de datos más reciente.

Recuerde: La serie de copia de seguridad más reciente de cualquiera de los dos tipos no se suprime.

Consulte el mandato MOVE DRMEDIA para obtener más información acerca de la caducidad de los volúmenes de copia de seguridad de la base de datos que no son volúmenes virtuales. Consulte el mandato EXPIRE INVENTORY para obtener más información acerca de la caducidad de los volúmenes de copia de seguridad de la base de datos que son volúmenes virtuales.

Utilice el mandato QUERY DRMSTATUS para ver el número de días especificado.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMDBBackupexpiredays--días-----<<
```

Parámetros

días (Obligatorio)

Especifica el número de días que debe transcurrir desde la creación de una serie de base de datos hasta que sea seleccionable para caducidad. El número de días debe coincidir con el período de retardo de reutilización de volúmenes para las agrupaciones de almacenamiento de copia que gestiona el gestor de recuperación ante siniestro. Especifique un valor entero de 0 a 9999.

Ejemplo: establecer la caducidad de la serie de copia de seguridad de la base de datos

Establecer el valor de caducidad de serie de copia de seguridad de base de datos en 60.

```
set drmdbbackupexpiredays 60
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMDBBACKUPEXPIREDAYS

Mandato	Descripción
DSMSERV RESTORE DB	Restaura una base de datos de IBM Spectrum Protect.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

Mandato	Descripción
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

SET DRMFILEPROCESS (Especificar el proceso de archivos)

Utilice este mandato para especificar si los mandatos MOVE DRMEDIA o QUERY DRMEDIA deben procesar los volúmenes de copia de seguridad de base de datos y los volúmenes de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE. Durante la instalación este valor se establece en NO. Utilice el mandato QUERY DRMSTATUS para determinar el valor actual.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

>>-Set DRMFILEProcess--+-No-- .
                        +-----+
                        +-No--+
                        '-Yes-'

```

Parámetros

No

Especifica que los mandatos MOVE DRMEDIA y QUERY DRMEDIA no procesan los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE. Este es el valor predeterminado.

Yes

Especifica que los mandatos MOVE DRMEDIA y QUERY DRMEDIA procesan los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE.

Ejemplo: especificar que los mandatos DRMEDIA no incluyan clases de dispositivo de tipo FILE

Establecer el valor del proceso de archivos en no.

```
set drmfileprocess no
```

Mandatos relacionados



Tabla 1. Mandatos relacionados con SET DRMFILEPROCESS


Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)

Utilice este mandato para especificar un prefijo para el nombre de archivo de instrucciones de recuperación. Si emite este mandato, IBM Spectrum Protect utilizará el prefijo especificado si el mandato PREPARE se ha emitido sin el prefijo INSTRPREFIX.

Utilice el mandato QUERY DRMSTATUS para visualizar el valor actual del prefijo.

 Sistemas operativos AIX  Sistemas operativos Linux El prefijo es el directorio de trabajo actual del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no se establece ningún prefijo, el prefijo se establece en el directorio que representa la instancia del servidor, que generalmente es el directorio desde donde se ha instalado el servidor originalmente.



Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMINSTRPrefix--prefijo-----<<
```

Parámetros

 Sistemas operativos AIX  Sistemas operativos Linux prefijo (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux

Especifica un prefijo de nombre de ruta para los archivos que contienen las instrucciones de recuperación. Al procesar el mandato PREPARE, IBM Spectrum Protect añade el nombre de la sección del archivo de plan de recuperación adecuado para buscar el archivo. La longitud máxima es de 250 caracteres.

El prefijo puede ser uno de los siguientes:

- **Ruta del directorio:** Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
/admsrv/recinstr/
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

- **Ruta del directorio seguida de una serie:** IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
/admsrv/recinstr/accounts
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```


- **Sólo serie:** IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado.
 - IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es /opt/tivoli/tsm/server/bin. Especifique lo siguiente:

```
shipping
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```

 Sistemas operativos Windows prefijo (Obligatorio)

 Sistemas operativos Windows

Especifica un prefijo de nombre de ruta para los archivos que contienen las instrucciones de recuperación. Al procesar el mandato PREPARE, IBM Spectrum Protect añade el nombre de la sección del archivo de plan de recuperación adecuado para buscar el archivo. La longitud máxima son 200 caracteres.

El prefijo puede ser uno de los siguientes:

- **Ruta del directorio:** Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
c:\admsrv\recinstr\
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

- **Ruta del directorio seguida de una serie:** IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
c:\admsrv\recinstr\accounts
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```



- **Sólo serie:** IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. La ruta del directorio es el directorio que representa a esta instancia del servidor de IBM Spectrum Protect (normalmente, el directorio de instalación original del servidor de IBM Spectrum Protect). Por ejemplo, el directorio que representa a esta instancia del servidor es c:\Archivos de programa\Tivoli\TSM;\server2 y se especifica el prefijo siguiente:

```
shipping
```


El nombre del archivo del plan de recuperación resultante es:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.19971115.051421
```

Ejemplo: especificar el prefijo del plan de recuperación

 Sistemas operativos AIX  Sistemas operativos Linux Especificar la lectura de las instrucciones del plan de recuperación del directorio /drmpln/primesrv.

```
set drminstrprefix /drmpln/primesrv/
```

 Sistemas operativos Windows Especificar la lectura de las instrucciones del plan de recuperación del directorio c:\win32app\ibm\adsm\server2\.

```
set drminstrprefix c:\win32app\ibm\adsm\server2\
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMINSTRPREFIX

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)

Utilice este mandato para especificar el nombre de la ubicación en el local para almacenar los medios. En la instalación, el nombre se establece en NOTMOUNTABLE. Utilice el mandato QUERY DRMSTATUS para ver el nombre de la ubicación.

El mandato MOVE DRMEDIA utiliza el nombre de la ubicación para establecer la ubicación de los volúmenes que se traspan al estado NOTMOUNTABLE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMNOTMountableName--ubicación-----<<
```

Parámetros

ubicación (Obligatorio)

Especifica el nombre de la ubicación en el local para almacenar los medios. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

Ejemplo: especificar el nombre de la ubicación en el local

Establecer el nombre de la ubicación en room 123/31.

```
set drmnotmountablename "room 123/31"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMNOTMOUNTABLERNAME

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)

Utilice este mandato para especificar un prefijo para un nombre de archivo del plan.

Si emite este mandato, IBM Spectrum Protect utilizará el prefijo especificado si el mandato PREPARE no incluye el parámetro PLANPREFIX.

Utilice el mandato QUERY DRMSTATUS para visualizar el valor actual del prefijo del plan de recuperación.



Clase de privilegio



Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMPLANPrefix--prefijo-----<<
```

Parámetros

 Sistemas operativos AIX  Sistemas operativos Linux prefijo (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el prefijo de un nombre de archivo de plan de recuperación.

La longitud máxima del prefijo son 250 caracteres. Si especifica una serie nula (""), el prefijo actual se elimina y el servidor utiliza el algoritmo que se describe en el parámetro PLANPREFIX del mandato PREPARE.

Para el prefijo, puede especificar:

- **Una ruta de directorio seguida de una barra inclinada (/):** IBM Spectrum Protect añade al prefijo la fecha y la hora en formato `aaaammdd.hhmmss`. Por ejemplo, SET DRMPLANPREFIX se ha establecido en lo siguiente:

```
/admsrv/recplans/
```

El nombre del archivo del plan de recuperación resultante es:

```
/admsrv/recplans/19971115.051421
```

- **Una ruta del directorio seguida de una serie:** IBM Spectrum Protect utiliza la serie como parte del nombre del archivo. IBM Spectrum Protect agrega al prefijo la fecha y la hora con el formato `.aaaammdd.hhmmss` (observe el punto inicial). Por ejemplo, SET DRMPLANPREFIX está establecido del modo siguiente:

```
/admsrv/recplans/accounting
```

El nombre de archivo del plan de recuperación resultante será:

```
/admsrv/recplans/accounting.19971115.051421
```

- **Una serie que no tiene antepuesta una ruta del directorio:** IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato `.aaaammdd.hhmmss` (observe el punto inicial). IBM Spectrum Protect determina la ruta del

directorio del modo siguiente:


- IBM Spectrum Protect utiliza el nombre de ruta del directorio de trabajo actual del servidor de IBM Spectrum Protect. Por ejemplo, el directorio de trabajo actual de IBM Spectrum Protect es /opt/tivoli/tsm/server/bin. El mandato SET DRMPLANPREFIX está establecido del modo siguiente:

```
shipping
```

El nombre del archivo del plan de recuperación resultante es:

```
/opt/tivoli/tsm/server/bin/shipping.19971115.051421
```

Sistemas operativos Windows prefijo (Obligatorio)

 Sistemas operativos Windows Especifica el prefijo del nombre de ruta que se utiliza para generar el nombre del archivo del plan de recuperación. El prefijo puede tener hasta 200 caracteres. IBM Spectrum Protect utiliza el prefijo si el mandato PREPARE se emite sin el parámetro PLANPREFIX. IBM Spectrum Protect crea un nombre de archivo de plan de recuperación exclusivo añadiendo al prefijo el formato de la fecha y la hora: aaaammdd.hhmmss (por ejemplo, 19951115.051421). Si especifica una serie nula (""), el prefijo actual se elimina y el servidor utiliza el algoritmo que se describe en el parámetro PLANPREFIX del mandato PREPARE.

Para el prefijo, puede especificar:

1. Una ruta de directorio
2. Una ruta de directorio seguida por una serie
3. Una serie

A continuación se describen las reglas de las especificaciones de prefijos posibles:

1. Para especificar una ruta de directorio para el prefijo, finalice el prefijo con una barra inclinada invertida (\). IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato aaaammdd.hhmmss. Por ejemplo, el mandato SET DRMPLANPREFIX se ha establecido de este modo:

```
c:\admsrv\recplans\
```

El nombre del archivo del plan de recuperación resultante es:

```
c:\admsrv\recplans\19951115.051421
```

Importante: Si emite el mandato SET DRMPLANPREFIX desde un cliente de línea de mandatos y el último carácter de la línea de mandatos es una barra inclinada invertida, IBM Spectrum Protect interpretará que se trata de un carácter de continuación. Para evitar esto, delimite el prefijo con comillas. Por ejemplo: "c:\admsrv\recplans\"

2. Si el prefijo es una ruta del directorio seguida de una serie, IBM Spectrum Protect utiliza la serie como parte del nombre de archivo. IBM Spectrum Protect agrega al prefijo la fecha y la hora con el formato .aaaammdd.hhmmss (observe el punto inicial). Por ejemplo, el mandato SET DRMPLANPREFIX se ha establecido de este modo:

```
c:\admsrv\recplans\accounting
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\admsrv\recplans\accounting.19951115.051421
```

3. Si el prefijo es una serie que no tiene delante una ruta, IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato .aaaammdd.hhmmss (observe el punto inicial). La ruta que IBM Spectrum Protect utiliza es la que representa a esta instancia del servidor de IBM Spectrum Protect (normalmente, el directorio desde donde se ha instalado originalmente el servidor de IBM Spectrum Protect). Por ejemplo, el directorio que representa esta instancia del servidor es c:\Archivos de programa\Tivoli\TSM;\server2, y decide establecer el prefijo en:




```
shipping
```

El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.19951115.051421
```

Ejemplo: especificar un prefijo para los nombres de archivo de plan de recuperación

Especificar un prefijo de modo que los archivos de plan de recuperación generados se almacenen en el directorio siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux/drmplan/primsrv
-  Sistemas operativos Windows c:\drmtest\prepare\

Emita el mandato:  Sistemas operativos AIX  Sistemas operativos Linux

```
set drmplprefix /drmplan/primsrv/
```

```
set drmplprefix c:\drmtest\prepare\
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMPLANPREFIX

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)

Utilice este mandato para especificar el carácter que se ha de agregar a los nombres de volúmenes de sustitución del archivo del plan de recuperación. El carácter puede ayudarle a localizar o generar los nombres de volúmenes de sustitución cuando utiliza el archivo del plan de recuperación.

Durante la instalación, el carácter se establece en @. IBM Spectrum Protect genera nombres de sustitución para los volúmenes de agrupación de almacenamiento primaria que el mandato DEFINE VOLUME ha añadido. Utilice el carácter agregado para:

- Localizar los nombres de volúmenes de sustitución en las secciones del plan de recuperación para poder cambiar los nombres en el momento de la recuperación. Por ejemplo, puede desconocer los nombres de los volúmenes de cinta disponibles en el local de recuperación.
- Generar los nombres de volúmenes de sustitución. Necesita un convenio de denominación que funcione para todos los tipos de dispositivo de las agrupaciones de almacenamiento primarias. Tenga en cuenta lo siguiente:
 - La longitud generada del nombre de volumen de sustitución
 - Los caracteres legales del nombre del volumen de sustitución
 - Los conflictos con nombres de volúmenes existentes
 - Los nombres de volumen de sustitución deben ser distintos de todos los nombres de volúmenes destruidos, existentes o nuevos.

Utilice el mandato QUERY DRMSTATUS para ver el carácter que se ha añadido al final de los nombres de los volúmenes de sustitución.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis


```
>>-Set DRMPLANVpostfix--carácter-----<<
```


Parámetros

carácter (Obligatorio)

Especifica el carácter que se agrega a los nombres de volúmenes de sustitución en el archivo de plan de recuperación.

Especifique un carácter alfanumérico o especial.

 Sistemas operativos AIXAtención: Un carácter especial puede ocasionar resultados imprevisibles en el shell o en el entorno de línea de mandatos de AIX.

 Sistemas operativos WindowsAtención: Un carácter especial puede ocasionar resultados imprevisibles en el proceso por lotes o en el entorno de línea de mandatos de Windows.

Ejemplo: especificar el carácter que ha de añadirse a los nombres de los volúmenes de sustitución

Establecer el carácter a agregar a los nombres de volumen de sustitución en R.

```
set drmplvpostfix R
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMPLANVPOSTFIX

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)

Utilice este mandato para especificar los nombres de las agrupaciones de almacenamiento primarias que desea recuperar. Si el mandato PREPARE no incluye el parámetro PRIMSTGPOOL, DRM procesará los nombres especificados en este mandato.

Utilice el mandato QUERY DRMSTATUS para que se visualicen los valores actuales. Durante la instalación, todas las agrupaciones de almacenamiento primarias definidas en el servidor se pueden seleccionar para el proceso de DRM.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```

      .-,------.
      v          |
>>-Set DRMPRIMstgpool----nombre_agrupación_primaria+----->>
  
```

Parámetros

nombre_agrupación_primaria (Obligatorio)

Especifica los nombres de las agrupaciones de almacenamiento primarias que desea recuperar. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Los nombres especificados sustituirán a los valores anteriores. Si especifica una serie nula (""), se eliminan todos los nombres actuales y se pueden seleccionar todas las agrupaciones de almacenamiento primarias para el proceso de DRM.

Ejemplo: establecer una agrupación de almacenamiento primaria que DRM ha de gestionar

Establecer en PRIMSTGPOOL1 la agrupación de almacenamiento primaria que ha de gestionar DRM.

```
set drmprimstgpool primstgpool1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMPRIMSTGPOOL

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.

SET DRMRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)

Utilice este mandato para especificar cuándo los archivos de planes de recuperación son seleccionables para caducarlos. Este mandato y el proceso de caducidad sólo se aplican a los archivos de plan de recuperación que se han creado con el parámetro DEVCLASS especificado en el mandato PREPARE (es decir, volúmenes virtuales de tipo RPFILe y RPSNAPSHOT). El proceso de caducidad del servidor de origen caduca los archivos de planes almacenados en el servidor de destino. Los archivos de planes de recuperación creados localmente no caducan.

Un archivo RPFILe está asociado con una serie de copia de seguridad de base de datos completa más las incrementales. Un archivo RPFSnapshot está asociado con una serie de copia de seguridad de instantánea de base de datos.

Atención: Los últimos archivos RPFILe y RPFSnapshot no se suprimen nunca.

Un archivo del plan recuperación es seleccionable para caducarlo si se cumplen las dos condiciones siguientes:

- El último archivo del plan de recuperación de la serie supera el valor de caducidad especificado con el mandato SET DRMRPFEXPIREDDAYS y el valor que se ha especificado para el parámetro DELgraceperiod en el mandato DEFINE SERVER. El valor predeterminado para el parámetro DELgraceperiod es de 5 días. Por ejemplo, si establece el valor para el mandato SET DRMRPFEXPIREDDAYS en 80 días y establece el valor para el parámetro DELgraceperiod en 6 días, el archivo de plan de recuperación no caduca hasta que han transcurrido 86 días.
- El último archivo del plan de recuperación no está asociado con la serie de copia de seguridad de base de datos más reciente.

Para obtener información acerca del proceso de caducidad, consulte el mandato EXPIRE INVENTORY.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set DRMRPFEXpiredays--días-----<<
```

Parámetros

días (Obligatorio)

Especifica el número de días que deben transcurrir para que caduque un archivo del plan de recuperación. Puede especificar un número de 0 a 9999. Durante la instalación, este valor se establece en 60.

Ejemplo: establecer la caducidad del plan de recuperación

Establecer el valor de caducidad del archivo del plan de recuperación en 30.

```
set drmrpfexpiredays 30
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMRPFEXPIREDDAYS

Mandato	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.
QUERY RPFILe	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

SET DRMVaultNAME (Especificar el nombre de la cámara de seguridad)

Utilice este mandato para especificar el nombre de la cámara de seguridad. En la instalación, el nombre se establece en Vault. Utilice el mandato QUERY DRMSTATUS para ver el nombre de la cámara de seguridad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET DRMVaultname--vault_name-----<<
```

Parámetros

nombre_cámara_seguridad (Obligatorio)

Especifica el nombre de la cámara de seguridad. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

Ejemplo: especificar un nombre de cámara de seguridad

Especificar `ironmountain` como nombre de la cámara de seguridad.

```
set drmvaultname ironmountain
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET DRMVaultNAME

Mandato	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)

Utilice este mandato para establecer el período de retención de los registros de eventos de la base de datos del servidor que le permitirá supervisar las planificaciones completadas. Se crea un registro de eventos cuando se arranca o falla el proceso de un mandato planificado.

Puede ajustar el período de tiempo durante el que el servidor mantiene la información de eventos para evitar datos insuficientes o caducados. El servidor elimina automáticamente de la base de datos los registros de eventos una vez transcurrido el período de retención y el margen de puesta en marcha del evento.

Puede emitir el mandato QUERY EVENT para que se visualice información acerca de los eventos planificados y que se han completado.

Puede emitir el mandato DELETE EVENT para suprimir registros de eventos, con independencia de si ha transcurrido o no el período de retención de éstos.

Puede emitir el mandato QUERY STATUS para que se visualice el valor del período de retención de eventos. Durante la instalación, este valor se establece en 10 días.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set EVentretention--días-----<<
```

Parámetros

días (Obligatorio)

El número de días que la base de datos retiene los registros de eventos. Puede especificar un entero de 0 a 9999. El valor 0 indica que sólo se retienen los registros de eventos del día actual.

Ejemplo: establecer el período de retención de los registros de eventos

Establecer el período de retención en 15 días.

```
set eventretention 15
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET EVENTRETENTION

Mandato	Descripción
DELETE EVENT	Elimina los registros de eventos antes de una fecha y hora especificadas.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)

Utilice este mandato para especificar la dirección IP que un cliente utiliza para conectarse a este servidor como el servidor de réplica secundario durante la migración tras error, si la dirección es diferente a la dirección IP que se ha especificado para el proceso de réplica.

Debe especificar la dirección del servidor que se utiliza si la dirección de alto nivel (HLA) es diferente. Este mandato solamente es necesario si se utilizan redes dedicadas para la comunicación entre servidores y el acceso de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET FAILOVERHladdress--dirección_alto_nivel-----><
```

Parámetros

dirección_alto_nivel (Obligatorio)

Especifica una dirección de alto nivel (HLA) de servidor como nombre decimal con puntos o nombre de host para utilizar durante la recuperación de errores. Si especifica un nombre de host, debe estar disponible un servidor que pueda resolver el nombre al formato decimal con puntos.

Para eliminar la dirección IP de migración tras error, emita el mandato sin especificar ningún valor.

Ejemplo: Establecer una dirección de alto nivel para la recuperación de errores

El nombre de la dirección de alto nivel que desea establecer para las operaciones de migración tras error en este servidor.

```
set failoverhladdress server1
```

Ejemplo: eliminar una dirección de alto nivel

Para eliminar una dirección de alto nivel de un servidor de migración tras error, emita el mandato siguiente:

```
set failoverhladdress
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con QUERY REPLSERVER

Mandato	Descripción
QUERY REPLSERVER (Consultar un servidor de réplica)	Muestra información sobre servidores de réplica.
REMOVE REPLSERVER (Eliminar un servidor de réplica)	Elimina un servidor de la réplica.

SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)

Utilice este mandato para establecer el número de intentos de conexión no válidos que se pueden realizar antes de bloquear un nodo.

El mandato SET INVALIDPWLIMIT también se aplica a los servidores de directorios LDAP que almacenan contraseñas complejas de nodos. Los servidores de directorios LDAP pueden limitar el número de intentos de contraseña no válidos independientemente del servidor de IBM Spectrum Protect. Es posible que no desee configurar el servidor de directorios LDAP para intentos no válidos para el espacio de nombres de IBM Spectrum Protect si utiliza el mandato SET INVALIDPWLIMIT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set--INVALIDPwlimit--number-----<<
```

Parámetros

número (Obligatorio)

Especifica el número de intentos no válidos permitidos antes de bloquear un nodo.

Puede especificar un entero de 0 a 9999. El valor 0 significa que no se comprueba el número de intentos de conexión no válidos. El valor 1 significa que si un usuario escribe una contraseña no válida una vez, el servidor bloquea el nodo. El valor predeterminado es 0.

Importante: Si la contraseña se almacena en un servidor de directorios LDAP, la puede gestionar el servidor LDAP y el servidor de IBM Spectrum Protect. No todos los mandatos del servidor de IBM Spectrum Protect afectan a las contraseñas que se autentican con un servidor LDAP. Por ejemplo, los mandatos SET PASSEXP y RESET PASSEXP no afectan a las contraseñas que se autentican con un servidor de directorios LDAP. Puede gestionar las características de contraseñas mediante el servidor de IBM Spectrum Protect. Si ha emitido el mandato SET INVALIDPWLIMIT, todas las contraseñas de IBM Spectrum Protect se controlan mediante el límite que establezca. Si configura el servidor de directorios LDAP para limitar el número de intentos de contraseña no válidos, puede producirse un conflicto.

Ejemplo: definir el número de intentos de conexión no válidos permitidos

Establecer el número de intentos de conexión no válidos permitidos.

```
set invalidpwlimit 6
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET INVALIDPWLIMIT

Mandato	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.

SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)

Utilice este mandato para definir una contraseña para el ID de usuario o cuenta especificado en el mandato SET LDAPUSER.

Requisito: Se debe definir la opción LDAPURL y emitir el mandato SET LDAPUSER antes de ejecutar el mandato SET LDAPPASSWORD. Si no está definida la opción LDAPURL cuando establece la contraseña de usuario para el servidor LDAP (Lightweight Directory Access Protocol), debe reiniciar el servidor de IBM Spectrum Protect después de definir la opción LDAPURL.

Clase de privilegio

Para emitir este mandato, debe tener privilegios del sistema.

Sintaxis

```
>>-Set LDAPPASSWORD--ldap_user_password-----<<
```

Parámetros

ldap_user_password

Especifica la contraseña que utiliza el servidor de IBM Spectrum Protect cuando se autentica con el servidor LDAP. La longitud máxima de la contraseña es de 64 caracteres. Si tiene signos de igual en su contraseña, la contraseña debe estar encerrada entre comillas. Se pueden utilizar los caracteres siguientes:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Ejemplo: Establecer una contraseña LDAP

```
set ldappassword LdAp20&12PaSsWoRd
```

Ejemplo: establecer una contraseña LDAP que incluya un signo igual

```
set ldappassword "LdAp=LastWoRd"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET LDAPPASSWORD

Mandato	Descripción
AUDIT LDAPDIRECTORY	Auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de directorios LDAP.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.

SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)

Utilice este mandato para especificar el ID de un usuario o cuenta que puede acceder a un servidor LDAP (Lightweight Directory Access Protocol).

El ID especificado debe tener acceso de lectura a las cuentas del servidor LDAP que se utilizan para la autenticación. Para modificar los ID o restaurar las contraseñas de los ID de LDAP, el ID de usuario o de cuenta especificado debe tener autorización para las cuentas del servidor LDAP.

Consejo: La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set LDAPUser--ldap_user_dn-----<<
```

Parámetros

ldap_user_dn
Especifica el ID de un usuario o cuenta que puede acceder a un servidor LDAP.

Ejemplo: Especifique un ID de usuario administrativo para realizar operaciones en un servidor LDAP.

Para especificar un administrador con un ID de usuario JACKSPRATT, que representa a una empresa de EE.UU, con el nombre EXAMPLE, emita el mandato siguiente:

```
set ldapuser JackSpratt@us.example.com
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET LDAPUSER

Mandato	Descripción
AUDIT LDAPDIRECTORY	Auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de directorios LDAP.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier mandato REGISTER NODE o REGISTER ADMIN.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.

SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)

Utilice este mandato para especificar el período, en días, entre las auditorías automáticas de licencias que realiza IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set--LICenseauditperiod--.-30---.  
+-----+-----<<  
'-días-'
```

Parámetros

días
Especifica el número de días entre auditorías automáticas de licencias. Este parámetro es opcional. El valor predeterminado es 30. Puede especificar un entero de 1 a 30, inclusive.

Ejemplo: especificar una auditoría de licencia de servidor de 14 días

Especificar que el servidor hace la auditoría de licencias cada 14 días.

```
set licenseauditperiod 14
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET LICENSEAUDITPERIOD

Mandato	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY AUDITOCCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.

SET MAXCMDRETRIES (Establecer el número máximo de reintentos de mandato)

Utilice este mandato para establecer el número máximo de veces que un planificador de un nodo cliente puede reintentar un mandato planificado que no se ha podido ejecutar.

Puede utilizar el mandato para modificar temporalmente el número máximo de reintentos que ha especificado el nodo cliente. El valor de un cliente se modifica temporalmente sólo si el cliente puede conectarse con el servidor.

Este mandato se utiliza con el mandato SET RETRYPERIOD para regular el período de tiempo y el número de reintentos que han de aplicarse a la reejecución de un mandato que no se ha realizado correctamente.

Puede emitir el mandato QUERY STATUS para visualizar el valor de reintentos actual. En la instalación, IBM Spectrum Protect se configura de modo que cada cliente determina su propio valor de reintentos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set MAXCMDRetries--+-+-----+-----<<
                    '-number-'
```

Parámetros

número

Especifica el número máximo de veces que el planificador de un nodo cliente puede reintentar un mandato planificado que no se ha podido ejecutar. Este parámetro es opcional.

El valor predeterminado es que cada cliente determina su propio valor para este parámetro. Puede especificar un entero de 0 a 9999. Consulte la documentación correspondiente al cliente para obtener más información sobre cómo establecer el número máximo de reintentos de mandatos del cliente.

Ejemplo: establecer el número máximo de reintentos de un mandato en 2

Reintentar, sólo dos veces, el intento fracasado de procesar un mandato planificado.

```
set maxcmdretries 2
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET MAXCMDRETRIES

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

Mandato	Descripción
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

SET MAXSCHEDESESSIONS (Establecer número máximo de sesiones planificadas)

Utilice este mandato para establecer el número de sesiones que el servidor puede utilizar para procesar operaciones planificadas. Este mandato especifica el número máximo de sesiones planificadas como porcentaje del número total de sesiones del servidor disponibles.

Al limitar el número de sesiones, se asegura que algunas de ellas estén disponibles para operaciones no planificadas, por ejemplo copia de seguridad o archivado. Puede aumentar el número total de sesiones (con el parámetro MAXSESSIONS) o el porcentaje máximo de sesiones planificadas. Sin embargo, si se aumenta el número total de sesiones disponibles, el rendimiento del servidor puede resultar afectado. Si se aumenta el porcentaje máximo de sesiones planificadas, se pueden reducir las sesiones disponibles para las operaciones sin planificar.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set MAXSCHedsessions--porcentaje-----<<
```

Parámetros

porcentaje (Obligatorio)

Especifica el porcentaje de sesiones totales del servidor que se puede utilizar para las operaciones planificadas. Puede especificar un entero de 0 a 100. El parámetro MAXSESSIONS del archivo de opciones de servidor determina el número máximo de sesiones de servidor totales disponibles.

Si establece el porcentaje máximo de sesiones planificadas en 0, no se pueden iniciar eventos planificados. Si establece el porcentaje máximo de sesiones planificadas en 100, el número máximo de sesiones planificadas es el valor de la opción MAXSESSIONS.

Consejo: Si el número máximo de sesiones planificadas no coincide con el porcentaje establecido en el mandato SET MAXSCHEDESESSIONS, ejecute el mandato SET MAXSCHEDESESSIONS otra vez. Compruebe la opción MAXSESSIONS y determine el número que se especifica. Si el número de la opción MAXSESSIONS ha cambiado y no ha emitido el mandato SET MAXSCHEDESESSIONS desde que se produjo el cambio, la cantidad máxima de sesiones planificadas puede cambiar.

Establecer un máximo de 20 sesiones para actividades planificadas

La opción MAXSESSIONS tiene el valor 80. Si desea que no haya más de 20 sesiones disponibles para la actividad planificada, establezca el porcentaje en 25.

```
set maxschedsessions 25
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET MAXSCHEDESESSIONS

Mandato	Descripción
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET MINPWLENGTH (Establecer longitud mínima de contraseña)

Utilice este mandato para establecer la longitud mínima de una contraseña.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set--MINPwlength--longitud-----<<
```

Parámetros

longitud (Obligatorio)

Especifica la longitud mínima de una contraseña. Puede especificar un entero de 0 a 64. El valor 0 significa que la longitud de la contraseña no se comprueba. El valor predeterminado para la longitud mínima de contraseña se establece en 0.

Ejemplo: establecer la longitud mínima de la contraseña

Establecer la longitud mínima de la contraseña en 5 caracteres.

```
set minpwlenght 5
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET MINPWLENGTH

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.

SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)

Utilice este mandato para establecer el grupo de servidores en los que se están supervisando las alertas y el estado. También puede utilizar este mandato para cambiar o eliminar el grupo de servidores supervisados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set MONITOREDSEVERGroup--+-----+-----<<  
      '-nombre_grupo-'
```

Parámetros

nombre_grupo

Especifica el nombre de grupo de servidores de IBM Spectrum Protect que contiene todos los servidores supervisados. Puede eliminar un nombre de grupo de servidores supervisados emitiendo el mandato sin especificar un valor o especificando un valor vacío (""). Finaliza cualquier supervisión existente de alertas y estado de los servidores remotos.

Establecer el nombre de un grupo de servidores supervisados

Establezca el nombre de un grupo de servidores supervisados SUBS, emitiendo el siguiente mandato:

```
set monitoredservergroup subs
```


Eliminar el nombre de un grupo de servidores supervisados

Elimine el grupo de servidores supervisados, emitiendo el mandato siguiente:

```
set monitoredservergroup
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET MONITOREDSEVERGROUP

Mandato	Descripción
DEFINE SERVERGROUP (Definir un grupo de nodo)	Define un nuevo grupo de servidores.
DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)	Define un servidor como miembro de un grupo de servidores.
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	Suprime un servidor de un grupo de servidores.
QUERY SERVERGROUP (Consultar un grupo de servidores)	Muestra información sobre grupos de servidores.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)	Establece el nombre del administrador de supervisión.

SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)

Utilice este mandato para establecer el nombre del administrador de supervisión que se utiliza para conectarse a los servidores del grupo de servidores supervisados.

Para visualizar el nombre del grupo de servidores supervisados, emita el mandato QUERY MONITORSETTINGS.

El nombre de administrador que especifique debe coincidir con el nombre de un administrador existente, de lo contrario, el mandato fallará.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set MONITORINGADMIN--+-+-----+-----<<  
                        '-nombre_admin-'
```

Parámetros

nombre_admin

Especifica el nombre de administrador. Puede eliminar nombres emitiendo el mandato sin especificar un valor o especificando un valor vacío ("").

Establecer el nombre de administrador de supervisión

Establezca el nombre del administrador de supervisión MONADMIN, emitiendo el siguiente mandato:

```
set monitoringadmin monadmin
```

Eliminar el nombre de administrador de supervisión

Elimine el administrador de supervisión, emitiendo el mandato siguiente:

```
set monitoringadmin ""
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET MONITORINGADMIN

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)	Establece el grupo de servidores supervisados.

SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)

Utilice este mandato para ajustar la modalidad de evaluación de riesgo de un nodo individual.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el dominio al que está asignado el nodo o bien autorización de propietario de cliente en el nodo.

Sintaxis

```
>>---Set NODEATRISKINTERVAL--nombre_nodo----->
>---TYPE-----+---DEFAULT-----+-----<
                +-BYPASSED-----+
                '-CUSTOM--Interval--==--valor-'
```

Parámetros

nombre_nodo (necesario)

Especifica el nombre del nodo cliente que desea actualizar..

TYPE (necesario)

Especifica el tipo de evaluación de riesgo. Especifique uno de los siguientes valores:

DEFAULT

Especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el mandato SET STATUSATRISKINTERVAL. El valor es cualquier sistema o aplicación, o VM y está determinado por el supervisor de estado.

Por ejemplo, puede especificar `TYPE = DEFAULT`, que permite que el supervisor de estado continúe y clasifique el nodo automáticamente. Entonces, el intervalo que se utiliza es el intervalo que se ha definido para dicha clasificación mediante el mandato SET STATUSATRISKINTERVAL.

BYPASSED

Especifica que el nodo no se evalúa para el estado de MV en riesgo por el supervisor de estado.. Se ha informado de que el estado de riesgo también es eludido en Centro de operaciones.

CUSTOM

Especifica que el nodo se evalúa con el intervalo que se ha especificado para el mandato SET STATUSATRISKINTERVAL.

Intervalo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. Debe especificar este parámetro cuando `TYPE = CUSTOM`. No especifique este parámetro cuando `TYPE = BYPASSED` o `TYPE = DEFAULT`. El valor de intervalo para todos los tipos de cliente se establece en 24 en la instalación del servidor.

Establecer nombre de nodo para utilizar un intervalo de riesgo personalizadas de 90 días

Establecer el intervalo de riesgo para un nodo denominado *fred* en 90 días.

```
set nodeatriskinterval fred type=custom interval=2160
```

Eludir la evaluación del intervalo de riesgo

Eluda la comprobación del intervalo de riesgo para un nodo denominado *bob*.

```
set nodeatriskinterval bob type=bypassed
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con set nodeatriskinterval

Mandato	Descripción
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)	Establece la modalidad de riesgo de un espacio de archivos de MV
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
QUERY NODE (Consultar nodos)	Visualiza información parcial o completa sobre uno o más clientes.
QUERY FILESPACE (Consultar uno o más espacios de archivos)	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.

SET PASSEXP (Establecer fecha de caducidad de contraseña)

Utilice este mandato para establecer el período de caducidad para las contraseñas de administrador y de nodo cliente. Puede establecer un período de caducidad común de contraseña para todas las contraseñas de administradores o de nodos de cliente, o bien puede establecer períodos de caducidad de contraseñas de forma selectiva.

Restricción: El mandato SET PASSEXP no se aplica a contraseñas que se autentican con un servidor de directorio LDAP.

Puede alterar temporalmente el valor SET PASSEXP para uno o varios nodos mediante el mandato REGISTER NODE o el mandato UPDATE NODE con el parámetro PASSEXP.

Los parámetros NODE o ADMIN deben especificarse para cambiar el período de caducidad de contraseñas de los nodos de cliente y los administradores con períodos de caducidad de contraseñas establecido de forma selectiva. Si no especifica los parámetros NODE o ADMIN, *todas* las contraseñas de nodos cliente y administradores utilizarán el nuevo período de caducidad de contraseña. Si de forma selectiva establece una caducidad de contraseña para un nodo o administrador que todavía no tiene establecido un período de caducidad de contraseña, no se modificará si posteriormente se establece la caducidad de contraseña para todos los usuarios.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set PASSExp--dias--+-----+----->
|                   .-,------. |
|                   v              | |
|'-Node-----nombre_nodo+--'
>--+-----+----->>
|                   .-,------. |
```

```
|      v      | |
'-Admin--=-----nombre_admin-+-'
```

Parámetros

días (Obligatorio)

Especifica el número de días que será válida una contraseña.

Puede especificar un número entre 1 y 9999 si no especifica el parámetro NODE o ADMIN. Si especifica el parámetro NODE o el parámetro ADMIN, puede especificar un número del 0 al 9999. El valor 0 significa que la contraseña no caduca nunca. Si caduca una contraseña, el servidor solicita una nueva contraseña cuando el administrador o el nodo de cliente se pone en contacto con el servidor.

Node

Especifica el nombre del nodo para el que desea establecer el período de caducidad de contraseña. Para especificar una lista de nodos, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Admin

Especifica el nombre del administrador cuyo período de caducidad de contraseña quiere establecer. Para especificar una lista de administradores, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Ejemplo: establecer la caducidad de la contraseña del administrador y del nodo de cliente

Establecer el período de caducidad de la contraseña de administrador o de nodo de cliente en 45 días.

```
set passexp 45
```

Ejemplo: establecer la caducidad de contraseña de un administrador

Establecer el período de caducidad de la contraseña del administrador LARRY en 120 días.

```
set passexp 120 admin=larry
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET PASSEXP

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)

Utilice el mandato SET PRODUCTOFFERING para definir la oferta de producto de IBM Spectrum Protect que tiene licencia para su empresa.

La definición se utiliza para determinar si IBM® License Metric Tool (ILMT) requiere cálculos de medida de capacidad de almacenamiento automático y si los tiene disponibles para su uso. Ejecute este mandato sólo si está utilizando ILMT para determinar el consumo de licencia.

Para las ofertas de productos donde ILMT tiene disponibles para su uso cálculos de medida de capacidad de almacenamiento automático, el parámetro también define qué enfoque de medida de capacidad se utiliza para esos cálculos.

El método de medición de capacidad se define en los términos de licencia de su oferta de producto específica. Para determinar la capacidad de almacenamiento calculada actualmente para su oferta de producto, consulte Verificación del cumplimiento de la licencia.

La misma información de capacidad de almacenamiento está disponible para ILMT semanalmente. Después de definir una oferta de producto aplicable utilizando este mandato, IBM Spectrum Protect realiza el cálculo de capacidad actual para esa oferta que está disponible para ILMT. Cuando se determina el cálculo de capacidad inicial que está disponible para ILMT, IBM Spectrum Protect actualiza el valor semanalmente.

Clase de privilegio

Para ejecutar este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET PRODUCTOFFERING--oferta_producto-----<<
```

Parámetros

oferta_producto (Obligatorio)

Especifica una oferta de producto. La longitud máxima de la serie de texto es de 255 caracteres. Las opciones siguientes están disponibles:

ENTry

Especifica que la oferta del producto con licencia en su empresa es IBM Spectrum Protect Entry. Esta oferta de producto utiliza una medida de licencia de tipo Per Managed Server. Las medidas de capacidad de esta oferta de producto no son aplicables.

DATARet

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect para retención de datos. Las medidas de capacidad para esta oferta de producto no se calculan automáticamente ni están disponibles para su uso en ILMT.

BASIC

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect. Esta oferta de producto utiliza una medida de licencia de processor value unit (PVU). Las medidas de capacidad de esta oferta de producto no son aplicables.

EE

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Extended Edition. Esta oferta de producto utiliza una medida de licencia de PVU. Las medidas de capacidad de esta oferta de producto no son aplicables.

SUIte

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

SUITEEntry

Especifica que la oferta del producto con licencia en su empresa es IBM Spectrum Protect Suite Entry. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

SUITEArchive

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - Archive. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

SUITEProtectier

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - ProtecTier. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

SUITEFrontend

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - FrontEnd. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

SUITEENTRYFrontend

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite Entry - FrontEnd. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

CLEAR

No se ha especificado ninguna oferta de producto.

Ejemplo: establecer la oferta de producto en IBM Spectrum Protect (BASIC)

```
set productoffering BASIC
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET PRODUCTOFFERING

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)

Utilice este mandato para regular la frecuencia con que los nodos cliente se ponen en contacto con el servidor para obtener el trabajo planificado cuando se ejecuta en la modalidad de planificación por sondeo de cliente.

Cada cliente puede establecer su propio período de reintentos en el momento en que se inicia su programa planificador. Puede utilizar este mandato para modificar temporalmente el valor que especifican todos los clientes que pueden conectarse con el servidor.

Si los nodos cliente sondean con mayor frecuencia para ver si hay planificaciones, los nodos reciben los cambios efectuados en las planificaciones con mayor rapidez. Sin embargo, si los nodos clientes aumentan el sondeo se aumenta también el tráfico de la red.

Puede emitir el mandato QUERY STATUS para que se visualice el valor del período establecido entre consultas de planificación. En la instalación, IBM Spectrum Protect se configura de modo que cada cliente determina su propio valor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set QUERYSchedperiod--+-+-----+----->>  
                        '-horas-'
```

Parámetros

horas

Especifica el número máximo de horas que el planificador de un nodo cliente espera entre intentos de ponerse en contacto con el servidor para obtener una planificación. Este parámetro es opcional. Puede especificar un entero de 1 a 9999. Si no especifica un valor para este parámetro, cada cliente determina su propio valor para este parámetro.

Ejemplo: establecer el período de sondeo para todos los nodos cliente

Hacer que todos los clientes que utilicen la modalidad de planificación por sondeo se pongan en contacto con el servidor cada 24 horas.

```
set querieschedperiod 24
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET QUERYSCHEDPERIOD

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.

SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)

Utilice este mandato para establecer las horas de inicio aleatorias en el margen de puesta en marcha de cada planificación para los clientes utilizando la modalidad de planificación por sondeo de cliente. El margen de puesta en marcha es la hora de inicio y la duración durante la que debe iniciarse la planificación. La modalidad de planificación por sondeo de cliente es una técnica de comunicaciones de cliente/servidor donde el cliente consulta el trabajo que hay al servidor.

Cada planificación cuenta con un margen de tiempo que indica durante qué período de tiempo puede llevarse a cabo su ejecución. Para equilibrar la carga de la red y del servidor, las horas de inicio para los clientes se pueden distribuir en dicho margen. Utilice este mandato para especificar la fracción del margen por la cual se distribuyen las horas de inicio para los clientes.

La aleatorización se produce al principio del margen para dejar tiempo para reintentos, si es necesario. Cuando la modalidad de planificación no se establece en sondeo, la aleatorización no se produce si el primer contacto del cliente con el servidor tiene lugar después de la hora de inicio del evento.

Puede emitir el mandato QUERY STATUS para que se visualice el valor del porcentaje de aleatorización de la planificación. En la instalación, el valor se establece en el 25 por ciento.

Establezca el porcentaje de aleatorización en un valor mayor que 0 para impedir errores de comunicaciones. Los errores de comunicaciones pueden producirse porque un gran grupo de clientes entra en contacto con el servidor simultáneamente. Si sufre errores de comunicaciones, puede aumentar el porcentaje de aleatorización, de modo que el contacto del cliente se distribuya. Con esto disminuyen las posibilidades de sobrecargas y errores en las comunicaciones.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set RANDomize--porcentaje-----<<
```

Parámetros

porcentaje (Obligatorio)

Especifica el porcentaje del margen de puesta en marcha sobre el que se distribuyen las horas de inicio de los clientes individuales. Puede especificar un entero de 0 a 50.

El valor 0 indica que no se produce ninguna aleatorización y que todos los clientes ejecutan las planificaciones al principio de los márgenes de tiempo de puesta en marcha.

El valor 50 indica que a los clientes se les asigna horas de inicio que se distribuyen aleatoriamente por la primera mitad de cada margen de puesta en marcha.

Durante la instalación, este valor es 25, lo cual indica que el primer 25 por ciento del margen de puesta en marcha se utiliza para la aleatorización.

Si ha especificado DURUNITS=INDEFINITE en el mandato DEFINE SCHEDULE, el porcentaje se aplica a un período de 24 horas. Por ejemplo, el valor 25% produciría un margen de 6 horas.

Ejemplo: establecer la aleatorización de las horas de inicio planificadas

Establecer la aleatorización en el 50 por cien.

```
set randomize 50
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET RANDOMIZE

Mandato	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.

SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)

Utilice este mandato para habilitar la recuperación en todo el sistema de archivos dañados a partir de un servidor de réplica de destino. Si este valor está activado, el proceso de réplica del nodo se puede configurar para detectar archivos dañados en el servidor de réplica de origen y sustituirlo por archivos sin dañar del servidor de réplica de destino.

El parámetro del sistema REPLRECOVERDAMAGED afecta a todos los procesos de recuperación de archivos en todos los procesos de réplica para todos los nodos y espacios de archivos. La recuperación de archivos sólo es posible si está instalado el software del servidor, Versión 7.1.1 o posterior, en los servidores de réplica de origen y destino, y si los datos del nodo se han replicado antes de que se dañaran los archivos.

Para visualizar el valor actual, utilice el mandato QUERY STATUS.

Cuando se instala el servidor, el valor predeterminado es ON.

Si actualiza el servidor y no se detectan archivos dañados, el valor predeterminado es ON.

Si actualiza el servidor y se detectan archivos dañados, el parámetro se establece en OFF y se emite un mensaje para indicar que la recuperación de archivos dañados se ha inhabilitado. El valor OFF impide que el servidor explore tablas de bases de datos en busca de objetos dañados que pueden recuperarse. La prevención de la exploración es necesaria en el caso de que se detecten muchos archivos dañados. En dicho caso, una exploración puede llevar bastante tiempo y debe planificarse cuando el uso de recursos del servidor se encuentra en un nivel mínimo. Cuando esté preparado para iniciar la exploración y recuperar los archivos dañados, debe emitir el mandato SET REPLRECOVERDAMAGED y especificar el valor ON. Una vez que el servidor finaliza satisfactoriamente la exploración, el parámetro del sistema REPLRECOVERDAMAGED se establece en ON.

En la tabla siguiente se describe cómo el parámetro de sistema REPLRECOVERDAMAGED y otros parámetros afectan a la recuperación de archivos dañados y replicados.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.

a medianoche. Por ejemplo, suponga que el período de retención es de dos días naturales. Si un proceso de réplica se completa a las 11:00 p.m. del día n , se retiene un registro de dicho proceso durante 25 horas hasta la medianoche del día $n+1$. Para visualizar el período de retención para los registros de réplica, emita el mandato QUERY STATUS en el servidor de réplica de origen.

Emita el mandato SET REPLRETENTION en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set REPLRETention--+.-----30-----+----->>
'-número_de_días-'
```

Parámetros

número_de_días (Obligatorio)

El número de días que el servidor de réplica de origen retiene los registros de réplica. Puede especificar un entero de 0 a 9999. El valor predeterminado es 30.

Ejemplo: establecer un período de retención para los registros de réplica de nodo de cliente

Desea retener los registros de réplica de nodo de cliente durante 10 días.

```
set replretention 10
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET REPLRETENTION

Mandato	Descripción
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET REPLSERVER (Establecer el servidor de réplica de destino)

Utilice este mandato para establecer el nombre de un servidor de réplica de destino. También puede utilizar este mandato para cambiar o eliminar un servidor de réplica de destino.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Para visualizar el nombre de un servidor de réplica de destino, emita el mandato QUERY STATUS en un servidor de réplica de origen.

Importante:

- El nombre de servidor que especifique con este mandato debe coincidir con el nombre de una definición de servidor existente. También debe ser el nombre del servidor que se utilizará como servidor de réplica de destino. Si el nombre de servidor especificado por este mandato no coincide con el nombre de servidor de una definición de servidor existente, el mandato falla.
- Tenga cuidado cuando cambie o elimine un servidor de réplica de destino. Si cambia un servidor de réplica de destino, los datos del nodo de cliente replicados se envían a un servidor de réplica de destino diferente. Si elimina un servidor de réplica de destino, los datos del nodo de cliente no se replican.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set REPLSERVER-----+-----<<  
      '-nombre_servidor_destino-'
```

Parámetros

nombre_servidor_destino

Especifica el nombre del servidor de réplica de destino. El nombre que especifique debe coincidir con el nombre de un servidor existente. La longitud máxima de un nombre es de 64 caracteres.

Para eliminar un servidor de réplica de destino, emita el mandato sin especificar ningún valor.

Nota: Si no desea continuar replicando datos, puede eliminar la configuración de réplica de nodo después de eliminar el servidor de réplica de destino.

Ejemplo: establecer un servidor de réplica de destino

El nombre del servidor que desea establecer como servidor de réplica de destino es SERVER1.

```
set replserver server1
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET REPLSERVER

Mandato	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
UPDATE SERVER	Actualiza la información sobre un servidor.
REMOVE REPLNODE	Elimina un nodo de la réplica.
REMOVE REPLSERVER	Elimina un servidor de la réplica.

SET RETRYPERIOD (Establecer período de tiempo entre reintentos)

Utilice este mandato para establecer el número de minutos que el planificador de un nodo cliente espera entre reintentos después de que haya fracasado un intento de ponerse en contacto con el servidor o de que un mandato planificado no se haya podido procesar.

Cada cliente puede establecer su propio período de reintentos en el momento en que se inicia su programa planificador. Puede utilizar este mandato para modificar temporalmente los valores que especifican todos los clientes que pueden conectarse con el servidor.

Este mandato se utiliza junto con el mandato SET MAXCMDRETRIES para regular el período de tiempo y el número de reintentos que han de aplicarse a la ejecución de un mandato que no se ha completado correctamente.

Puede emitir el mandato QUERY STATUS para que se visualice el valor del período establecido entre reintentos. En la instalación, IBM Spectrum Protect permite que cada cliente determine su propio período entre reintentos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set RETRYPeriod--+-----+----->>
      '-minutos-'
```

Parámetros

minutos

Especifica el número de minutos que el planificador de un nodo cliente espera entre reintentos después de que haya fracasado un intento de contactar al servidor o de que un mandato planificado no se haya podido procesar. Al establecer el período entre reintentos, establezca un período de tiempo que permita más de un reintento en un margen de puesta en marcha normal. Puede especificar un entero de 1 a 9999.

Ejemplo: establecer un período de tiempo de quince minutos entre reintentos

Establecer que el planificador cliente vuelva a intentar cada quince minutos el establecimiento de contacto con el servidor o el proceso de los mandatos planificados que no se han ejecutado correctamente.

```
set retryperiod 15
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET RETRYPERIOD

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un mandato planificado.

SET SCHEDMODES (seleccionar modalidad de planificación central)

Utilice este mandato para determinar cómo se comunican los clientes con el servidor para comenzar el trabajo planificado. Cada cliente debe configurarse para seleccionar la modalidad de planificación en la que opera.

Utilice este mandato con el mandato SET RETRYPERIOD para regular el período de tiempo y el número de reintentos de proceso que han de aplicarse a un mandato que no se ha ejecutado correctamente.

Puede emitir el mandato QUERY STATUS para que se visualice el valor de la modalidad de planificación que recibe soporte. En la instalación, este valor es ANY.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SCHEDMODEs--+ANY-----+----->>
      +-Polling--+
      '-PRompted-'
```

Parámetros

ANY

Especifica que los clientes pueden ejecutar la modalidad de planificación por sondeo de cliente o por petición de servidor.

Polling

Especifica que únicamente puede utilizarse la modalidad de planificación por sondeo de cliente. Los nodos de cliente sondean el servidor en intervalos de tiempo especificados para obtener el trabajo planificado.

PRompted

Especifica que únicamente puede utilizarse la modalidad de planificación por petición de servidor. Esta modalidad únicamente está disponible para los clientes que se comunican a través de TCP/IP. Los nodos de cliente esperan a que el servidor se ponga en contacto con ellos cuando se ha de realizar el trabajo planificado y hay una sesión disponible.

Ejemplo: limitar las operaciones planificadas para los clientes con el sondeo por cliente

Los clientes pueden ejecutar la planificación central por petición de servidor y por sondeo de cliente. Suponga que se desea limitar temporalmente las operaciones planificadas a los clientes que utilicen la modalidad de planificación por sondeo de cliente. Si establece la modalidad de planificación en POLLING, el servidor dejará de solicitar a los clientes que ejecuten los mandatos planificados. Esto significa que cualquier planificador cliente que utilice la modalidad de planificación por petición de servidor esperará hasta que establezca la modalidad de planificación en ANY o PROMPTED.

```
set schedmodes polling
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SCHEDMODES

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

SET SCRATCHPADRETENTION (Establecer hora de retención de registro)

Utilice este mandato para establecer la cantidad de tiempo para la que se retienen entradas de registro.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SET SCRATCHPADRETENTION--días-----<<
```

Parámetros

días (Obligatorio)

Especifica el número de días que una entrada de registro se retiene después de la última actualización en la entrada de registro. Puede especificar un entero en el rango 1 – 9999.

Ejemplo: retener entradas de registro para 367 días después de que se actualicen

```
set scratchpadretention 367
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET SCRATCHPADRETENTION

Mandato	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)

Utilice este mandato para establecer la dirección de alto nivel (IP) de un servidor. IBM Spectrum Protect utiliza la dirección cuando se emite un mandato DEFINE SERVER con CROSSDEFINE=YES. Es necesario utilizar el mandato SET SERVERHLADDRESS para todos los despliegues automáticos de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SERVERHladdress--dirección_ip-----<<
```

Parámetros

dirección_ip (Obligatorio)

Especifica la dirección de alto nivel como un nombre numérico decimal con puntos o como un nombre de host. Si se especifica un nombre de host, debe haber disponible un servidor que pueda resolver el nombre con el formato decimal con puntos.

Ejemplo: establecer la dirección de alto nivel de un servidor

Establecer la dirección de alto nivel de HQ_SERVER en 9.230.99.66.

```
set serverhladdress 9.230.99.66
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SERVERHLADDRESS

Mandato	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.

SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)

Utilice este mandato para establecer la dirección de bajo nivel de un servidor. IBM Spectrum Protect utiliza la dirección cuando se emite un mandato DEFINE SERVER con CROSSDEFINE=YES.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SERVERLladdress--puerto_tcp-----<<
```

Parámetros

puerto_tcp (Obligatorio)

Especifica la dirección de bajo nivel del servidor. Por lo general, esta dirección es idéntica a la de la opción TCPPOINT del archivo de opciones del servidor.

Ejemplo: establecer la dirección de bajo nivel de un servidor

Establecer la dirección de bajo nivel de HQ_SERVER en 1500.

```
set serverlladdress 1500
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SERVERLLADDRESS

Mandato	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.

SET SERVERNAME (Especificar el nombre del servidor)

Utilice este mandato para cambiar el nombre del servidor. Cuando instala el servidor de IBM Spectrum Protect, el nombre se establece durante la instalación en SERVER1.

Utilice el mandato QUERY STATUS para que se visualice el nombre del servidor.

Si migra desde ADSM hasta IBM Spectrum Protect, el nombre se establece en ADSM o en el último nombre que se ha especificado para ADSM con el mandato SET SERVERNAME.

Importante:

- Si es un servidor origen para una operación de volúmenes virtuales, el cambio del nombre puede afectar a la capacidad del servidor origen de acceder a los datos almacenados en el servidor destino correspondiente y gestionarlos.
- Para evitar que se produzcan problemas relacionados con la propiedad de los volúmenes, no cambie el nombre de un servidor si es un cliente de biblioteca.

Al cambiar el nombre de un servidor, tenga en cuenta las restricciones adicionales siguientes:

- Los clientes de Windows utilizan el nombre del servidor para identificar qué contraseñas pertenecen a qué servidores. El cambio del nombre del servidor después de que los clientes se hayan conectado dará lugar a que los clientes deban volver a especificar forzosamente las contraseñas.
- Debe establecer nombres exclusivos en los servidores que se comunican entre sí. En una red donde los clientes se conectan a múltiples servidores, es recomendable que todos ellos tengan nombres exclusivos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SERVERname--nombre_servidor-----<<
```

Parámetros

nombre_servidor (Obligatorio)

Especifica el nuevo nombre del servidor. El nombre debe ser exclusivo en toda la red de servidores para la anotación de eventos de empresa, la configuración de empresa, el direccionamiento de mandatos o los volúmenes virtuales. La longitud máxima del nombre es de 64 caracteres.

Ejemplo: especificar el nombre de un servidor

Dar al servidor el nombre WELLS_DESIGN_DEPT.

```
set servername wells_design_dept
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SERVERNAME

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET SERVERPASSWORD (Establecer contraseña de servidor)

Utilice este mandato para establecer la contraseña de las comunicaciones entre servidores para dar soporte a la administración de empresa y a el registro de eventos y supervisión de empresa.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SERVERPAssword--contraseña-----<<
```

Parámetros

contraseña (Obligatorio)

Especifica la contraseña del servidor. Los demás servidores deben tener la misma contraseña en las definiciones de este servidor.

Ejemplo: establecer la contraseña de un servidor

Establecer la contraseña de HQ_SERVER en agave.

```
set serverpassword agave
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SERVERPASSWORD

Mandato	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.

SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)

Utilice este mandato para establecer la regla de réplica del servidor de los datos gestionados por espacio.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos gestionados por espacio se establecen en DEFAULT.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Puede especificar una regla de réplica de prioridad normal o una regla de réplica de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos gestionados por espacio y datos de copia de seguridad. La réplica de los datos gestionados por espacio tiene una prioridad más alta que los datos de copia de seguridad. Para dar prioridad a los datos gestionados por espacio, emita el mandato SET SPREPLRULEDEFAULT y especifique la regla de réplica ALL_DATA_HIGH_PRIORITY. Para priorizar los datos de copia de seguridad, emita el mandato SET BKREPLRULEDEFAULT y especifique la regla de réplica ALL_DATA para los datos de copia de seguridad. La regla ALL_DATA para los datos de copia de seguridad replica los datos de copia de seguridad con una prioridad normal.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SPREPLRuledefault---ALL_DATA-----+-----<<
```



```
--ALL_DATA_HIGH_PRIORITY--
'-NONE-----'
```

Parámetros

ALL_DATA
Hace una réplica de los datos gestionados por espacio con una prioridad normal.

ALL_DATA_HIGH_PRIORITY
Hace una réplica de los datos gestionados por espacio con una prioridad alta.

NONE
Los datos gestionados por espacio no se replican.

Ejemplo: establecer la regla de réplica del servidor para los datos gestionados por espacio

Configure la regla predeterminada para que los datos gestionados por espacio se repliquen con una prioridad alta.

```
set spreplruledefault all_data_high_priority
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET BKREPLRULEDEFAULT

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)

Utilice este mandato para ajustar el intervalo de actividad de copia de seguridad que se utiliza cuando el supervisor de estado valora si los clientes están en peligro.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>---Set STATUSATRISKINTERVAL--TYPE-------+--All-----+----->
                                     +-Applications+-
```

```
+--VM-----+
'-Systems-----'
```

```
>----Interval---valor-----<<
```

Parámetros

TYPE (necesario)

Especifica el tipo de cliente que debe evaluarse. Especifique uno de los siguientes valores:

ALL

Especifique este valor para todos los tipos de cliente.

Applications

Especifique este valor sólo para tipos de cliente de aplicación.

VM

Especifique este valor para tipos de clientes de sistemas virtuales.

Systems

Especifique este valor para los tipos de cliente de sistemas.

Interval (Necesario)

Especifica la cantidad de tiempo, en horas, entre la actividad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. El valor de intervalo para todos los tipos de cliente se establece en 24 en la instalación del servidor.

Establecer que los sistemas utilicen un intervalo de dos semanas de en peligro

Establezca la comprobación de intervalo de en peligro para los tipos de cliente de sistemas en 2 semanas.

```
set statusriskinterval type=systems interval=336
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)

Utilice este mandato para habilitar e inhabilitar la supervisión de estado. La activación de la supervisión de estado por primera vez también establece los valores de umbral predeterminados y aumenta la retención de registros de sucesos hasta 14 días como mínimo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set STATUSREFreshinterval--minutos-----><
```

Parámetros

minutos (Necesario)

Especifica el número aproximado de minutos entre consultas de servidor de supervisión. Puede especificar un entero en el rango 1 – 2440. El valor predeterminado es 5.

Restricciones:

- En un entorno de almacenamiento supervisado por el Centro de operaciones, establezca el mismo intervalo de renovación en los servidores de concentrador y spoke. Si utiliza intervalos diferentes, el Centro de operaciones puede mostrar información inexacta para los servidores spoke.
- Los intervalos cortos de renovación de estado utilizan más espacio en la base de datos de servidor y pueden necesitar más recursos de procesador y de disco. Por ejemplo, disminuir el intervalo por la mitad duplica el espacio necesario de base de datos y de registro de archivado. Los intervalos largos reducen la actualidad de los datos del Centro de operaciones, pero se ajustan mejor a una configuración de red de alta latencia.
- Un intervalo de renovación de estado de menos de 5 minutos puede producir los problemas siguientes:
 - Los datos del Centro de operaciones que se supone se han de renovar después del intervalo definido tardan mucho más tiempo en renovarse.
 - Los datos del Centro de operaciones que se supone se han de renovar casi inmediatamente después de que se produzca un cambio relacionado en el entorno de almacenamiento también tardan más tiempo en renovarse.

Establecer el intervalo de renovación para la supervisión de estado

Especifique que el estado de servidor se consulte cada 6 minutos, emitiendo el mandato siguiente:

```
set statusrefreshinterval 6
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET STATUSREFRESHINTERVAL

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)

Utilice este mandato para hacer que el supervisor de estado considere a los clientes como en riesgo cuando evalúe el estado para cada cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set STATUSSKIPASFAILURE--+-Yes-+----->
                               '-No--'

>--TYPE-----+All-----<<
                +-Applications-+
                +-VM-----+
                '-SYstems-----'
```

Parámetros

State (Necesario)

Especifica si se habilitará la comprobación de los archivos omitidos durante la última copia de seguridad. Esta comprobación significa que el cliente está en riesgo si se ha omitido algún archivo. Los datos de cliente que se han omitido o de los que no se ha realizado una copia de seguridad correcta se consideran en riesgo.

Yes

Especifica que el servidor evalúa si un cliente está en riesgo.

No

Especifica que el servidor no evalúa si un cliente está en riesgo.

TYPE (necesario)

Especifica el tipo de cliente que debe evaluarse. Especifique uno de los siguientes valores:

ALL

Especifique este valor para todos los tipos de cliente.

Applications

Especifique este valor sólo para tipos de cliente de aplicación.

VM

Especifique este valor para tipos de clientes de sistemas virtuales.

SYstems

Especifique este valor para los tipos de cliente de sistemas.

Inhabilitar la evaluación de en riesgo para los tipos de cliente de sistema virtual

Ejecute el siguiente mandato para inhabilitar la evaluación de en riesgo para los tipos de cliente de sistemas virtuales:

```
set statusskipasfailure off type=vm
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET STATUSSKIPASFAILURE

Mandato	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.

Mandato	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)

Utilice este mandato para configurar el servidor para que los clientes puedan hacer copias de seguridad de subarchivos. En la estación de trabajo del cliente, las opciones SUBFILECACHEDPATH y SUBFILECACHESIZE deben especificarse en el archivo de opciones del cliente (dsm.opt). Si utiliza un cliente Windows, también debe especificar la opción SUBFILEBACKUP.

Con las copias de seguridad de subarchivos, cuando anteriormente se ha realizado la copia de seguridad de un archivo del cliente, la realización de las copias de seguridad posteriores normalmente se aplica a la parte (un subarchivo) del archivo del cliente que ha cambiado, en lugar de aplicarse al archivo completo.

Utilice el mandato QUERY STATUS para determinar si puede realizarse la copia de seguridad de los subarchivos en el servidor que ejecuta este mandato.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SUBFILE---Client+-----><
                '-No-----'
```

Parámetros

Client

Especifica que el nodo cliente puede determinar si desea utilizar la copia de seguridad de subarchivos.

No

Especifica que las copias de seguridad de subarchivos no se utilizarán. Durante la instalación, este valor se establece en No.

Ejemplo: establecer la realización de la copia de seguridad de los subarchivos para los nodos cliente

Permitir que el nodo cliente realice copias de seguridad de subarchivos en el servidor.

```
set subfile client
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET SUBFILE

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)

Utilice este mandato para especificar el número de días que se debe mantener la información en la tabla resumen de actividades SQL.

La tabla resumen de actividades SQL contiene estadísticas sobre cada sesión de cliente y los procesos del servidor. Para obtener una descripción de la información que contiene la tabla resumen de actividades SQL, emita el siguiente mandato:

```
select colname, remarks from columns where tabname='SUMMARY'
```

Emita el mandato QUERY STATUS para visualizar el número de días que ha de conservarse la información. Durante la instalación, IBM Spectrum Protect permite que cada servidor determine su propio número de días que debe mantener la información en la tabla resumen de actividades SQL.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set SUMmaryretention--+-+-----+----->><
                               '-días-'
```

Parámetros

días

Especifica el número de días que se debe mantener la información en la tabla resumen de actividades. Puede especificar un número comprendido entre 0 y 9999. El valor 0 significa que no se mantiene información en la tabla resumen de actividades. Un valor de 1 especifica que se debe mantener la tabla resumen de actividades durante el día de hoy.

Ejemplo: especificar el número de días que ha de conservarse la información en la tabla resumen de actividades SQL

Establecer el servidor para que retenga la información de la tabla resumen de actividades durante 15 días.

```
set summaryretention 15
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET SUMMARYRETENTION

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
SELECT	Permite las consultas personalizadas de la base de datos de IBM Spectrum Protect.

SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)

Utilice este mandato para permitir al servidor de IBM Spectrum Protect anotar las notificaciones de la información de diagnóstico de los dispositivos de unidad y biblioteca. Durante la instalación, este valor se establece en OFF. Si se activan, el servidor puede recuperar información de diagnóstico de un dispositivo de cinta o biblioteca y visualizarla mediante mensajes ANR. Si se desactivan, el servidor no consultará ningún dispositivo para obtener esta información.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-Set TAPEAlertmsg--+-ON--+-----><
      '-OFF-'
```

Parámetros

- ON
Especifica que la información de diagnóstico se reportará al servidor.
- OFF
Especifica que la información de diagnóstico no se reportará al servidor.

Ejemplo: activar los mensajes de alerta de cinta

Permitir que el servidor reciba mensajes de la información de diagnóstico.

```
set tapealertmsg on
```

Mandatos relacionados

Tabla 1. Mandato relacionado con SET TAPEALERTMSG

Mandato	Descripción
QUERY TAPEALERTMSG	Visualiza si el servidor anota la información de diagnóstico de hardware.

SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)

Utilice este mandato para especificar el número de minutos aproximado que los datos de tabla de contenido sin referencia permanecerán cargados en la base de datos del servidor.

En las operaciones de copia de seguridad controladas por NDMP de los sistemas de archivos NAS, el servidor puede recopilar información sobre los archivos y directorios de la imagen y almacenar esta información en una tabla de contenido dentro de una agrupación de almacenamiento. Se puede emplear el cliente web para examinar los archivos y directorios de una o varias imágenes de sistema de archivos visualizando las entradas de los datos de la tabla de contenido. El servidor carga los datos necesarios de la tabla de contenido en una tabla de base de datos temporal.

Una vez cargados los datos, el usuario puede seleccionar los archivos y directorios que se restaurarán. Como esta tabla de base de datos es temporal, los datos sólo permanecerán cargados durante un período de tiempo específico desde la última referencia a esos datos. Durante la instalación, el tiempo de retención se establece en 120 minutos. Utilice el mandato QUERY STATUS para ver el tiempo de retención de carga de la tabla de contenido.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-Set TOCLOADRetention--minutos-----><
```

Parámetros

- minutos (Obligatorio)
Especifica el número de minutos aproximado que los datos de tabla de contenido sin referencia se conservan en la base de datos. Puede especificar un entero de 30 a 1000.

Ejemplo: definir el período de retención de carga para la tabla de contenido

Utilizar el mandato SET TOCLOADRETENTION para especificar que los datos de la tabla de contenido sin referencia deben conservarse en la base de datos durante 45 minutos.

```
set toclloadretention 45
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SET TOCLOADRETENTION

Mandato	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.

SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)

Utilice este mandato para ajustar la modalidad de evaluación de riesgo para un espacio de archivos de la máquina virtual individual.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el domino al que está asignado el nodo o bien autorización de propietario de cliente en el nodo.

Sintaxis

```
>>---Set VMATRISKINTERVAL--nombre_nodo--fsid----->
>---TYPE-----+---DEFAULT---+-----+-----<
      +-BYPASSED+  '-Interval---valor-'
      '-CUSTOM---'
```

Parámetros

nombre_nodo (necesario)

Especifica el nombre del nodo de cliente que posee el espacio de archivo de máquina virtual que desea actualizar.

fsid (necesario)

Especifica el ID de espacio de archivos del nodo cliente que desea actualizar.

TYPE (necesario)

Especifica qué modalidad de evaluación de riesgo el supervisor de estado debe utilizar al evaluar la clasificación de riesgo del espacio de archivos de MV de los nodos especificados. Especifique uno de los siguientes valores:

DEFAULT

Especifica que el espacio de archivos de la máquina virtual se evalúa con el mismo intervalo que se ha especificado para el mandato SET STATUSATRISKINTERVAL.

BYPASSED

Especifica que el espacio de archivos no se evalúa para el estado de MV en riesgo por el supervisor de estado. Se ha informado de que el estado de riesgo también es eludido en Centro de operaciones.

CUSTOM

Especifica que el espacio de archivos de la máquina virtual se evalúa con el intervalo que se ha especificado para el mandato SET STATUSATRISKINTERVAL.

Intervalo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. Debe especificar este parámetro cuando TYPE = CUSTOM. No especifique este parámetro cuando TYPE = BYPASSED o TYPE = DEFAULT. El valor de intervalo para todos los tipos de cliente se establece en 24 en la instalación del servidor.

Establecer nombre de nodo para utilizar un intervalo de riesgo personalizadas de 90 días

Definir el intervalo de riesgo de uno nodo denominado *charlievm* (ID de espacio de archivos 50) en un nodo de centro de datos denominado *alice* para utilizar un intervalo de riesgo de 90 días. Puede emitir el mandato QUERY FILESPACE para determinar el ID de

espacio de archivos de la MV.

```
set vmatriskinterval alice 50 type=custom interval=2160
```

Eludir la evaluación del intervalo de riesgo

Excluir la MV llamada *davevm* (ID de espacio de archivos 213) en el nodo de datos denominado *erin* de la comprobación de intervalo de peligro. Puede emitir el mandato QUERY FILESPACE para determinar el ID de espacio de archivos de la MV denominada *davevm*. A continuación, establezca la comprobación del intervalo de riesgo para la MV en eludido.

```
set vmatriskinterval erin 213 type=bypassed
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con set vmatriskinterval

Mandato	Descripción
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)	Establece la modalidad y el intervalo de riesgo de un nodo
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
QUERY NODE (Consultar nodos)	Visualiza información parcial o completa sobre uno o más clientes.
QUERY FILESPACE (Consultar uno o más espacios de archivos)	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.

SETOPT (Establecer una opción de servidor para actualización dinámica)

Puede utilizar el mandato SETOPT para actualizar la mayoría de las opciones de servidor dinámicamente sin detener y reiniciar el servidor. Para la opción DBDIAGLOGSIZE, debe detener e iniciar el servidor. Un mandato SETOPT que esté en una macro o en un script no se puede retrotraer.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SETOPT--nombre_opción--valor_opción----->>
```

Parámetros

nombre_opción (Obligatorio)

Especifica un texto informativo que identifica la opción del servidor que se actualiza. La longitud máxima de la serie de texto es de 255 caracteres. Las opciones siguientes están disponibles:

- ADMINCOMMTIMEOUT
- ADMINIDLETIMEOUT

- ALLOWREORGINDEX
- ALLOWREORGTABLE
- ARCHLOGCOMPRESS
- BACKUPINITIATIONROOT
- CHECKTAPEPOS
- CLIENTDEDUPTXNlimit
- CLIENTDEPLOYCATALOGURL
- CLIENTDEPLOYUSELOCALCATALOG
- COMMTIMEOUT
-  Sistemas operativos Windows DATEFORMAT
- DBDIAGLOGSize
- DBDIAGPATHFSTHreshold
- DEDUPTIER2FILESIZE
- DEDUPTIER3FILESIZE
- DEDUPREQUIRESBACKUP
- DNSLOOKUP
- EXPINTERVAL
- EXPQUIET
- FSUSEDTHreshold
- IDLETIMEOUT
- LDAPCACHEDURATION
- MAXSESSIONS
- MOVEBatchsize
- MOVESIZETHRESHOLD
- NDMPPREFDATAINTERFACE
-  Sistemas operativos Windows NUMBERFORMAT
- NUMOPENVOLSAILOWED
- RECLAIMDELAY
- RECLAIMPERIOD
- REORGBEGINTIME
- REORGDURATION
- RESOURCETIMEOUT
- RESTOREINTERVAL
- RETENTIONEXTENSION
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANDISCOVERY
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANREFRESHTIME
- SERVERDEDUPTXNlimit
- SHREDding
-  Sistemas operativos Windows TCPPORT
- THROUGHPUTDATAthreshold
- THROUGHPUTTIMETHRESHOLD
-  Sistemas operativos Windows TIMEFORMAT
- TXNGROUPMAX

valor_opción (Obligatorio)

Especifica el valor de la opción del servidor.

Ejemplo: establecer el número máximo de sesiones de cliente

Actualice a 40 la opción del servidor para el número máximo de sesiones de clientes.

```
setopt maxsessions 40
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SETOPT

Mandato	Descripción
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY SYSTEM	Muestra detalles sobre el sistema servidor de IBM Spectrum Protect.

SHRED DATA (destruir datos)

esta opción únicamente después de que el servidor haya notificado errores de E/S durante la destrucción de datos y no pueda corregir el error.

Ejemplo: destruir datos

Iniciar manualmente la destrucción de todos los datos confidenciales suprimidos. Permitir que la ejecución del proceso continúe durante seis horas como máximo antes de que tenga lugar la cancelación automática de éste.

```
shred data duration=360
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SHRED DATA

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.

SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)

Utilice este mandato para suspender una operación de exportación de servidor a servidor que tiene un valor de FILEDATA que no es NONE. La operación de exportación que desea suspender debe haber pasado la fase de inicialización para poder considerarse seleccionable para la suspensión. El estado de la operación de exportación se guarda. La operación puede reiniciarse mediante la emisión del mandato RESTART EXPORT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-SUSPend EXPORT +-----<<
                    .-*-----
                    +-----+-----<
                    '---identificador_exportación---'
```

Parámetros

EXPORTIdentifier

Este parámetro opcional especifica el nombre de la operación de exportación. Puede buscar un nombre emitiendo el mandato QUERY EXPORT para que se muestren todas las operaciones de exportación de servidor a servidor que se están ejecutando en ese momento y se pueden suspender. También puede utilizar el carácter comodín para especificar el nombre.

Ejemplo: suspender una operación de exportación específica

Suspender la operación de exportación en EXPORTALLACCTNODES en ejecución. Cuando se emite el mandato SUSPEND EXPORT, no se genera ninguna salida. Debe emitir el mandato QUERY EXPORT para verificar que la operación EXPORTALLACCTNODES se ha suspendido.

```
suspend export exportallacctnodes
```

Ejemplo: suspender todas las operaciones de exportación en ejecución

Suspender todas las operaciones de exportación con el estado RUNNING.

```
suspend export *
```

Mandatos relacionados

Ejemplo: desbloquear todos los ID de usuario administrador que autentican contraseñas con un servidor de directorios LDAP

El ID de usuario administrador que utiliza contraseñas para autenticarse con un servidor de directorios LDAP debe estar bloqueado para que los ID puedan comunicarse con el servidor de IBM Spectrum Protect .

```
unlock admin * authentication=ldap
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UNLOCK ADMIN

Mandato	Descripción
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.

UNLOCK NODE (Desbloquear un nodo cliente)

Utilice este mandato para permitir que un nodo bloqueado tenga acceso al servidor. También puede desbloquear varios nodos que utilizan el mismo método de autenticación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-UNLOCK Node---*-----+--+-----+-----+-----+-----+<<
      '-nombre_nodo-'   '-AUTHentication-----+Local+-'
                          '-LDap--'
```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se desbloquea. Puede utilizar caracteres comodín para especificar el nombre de nodo. No tiene que especificar un nombre de nodo, si desea desbloquear todos los nodos de acuerdo con su método de autenticación. Utilice el comodín con un método de autenticación para desbloquear grupos de nodos. Este parámetro es obligatorio. No hay ningún carácter comodín de forma predeterminada.

AUTHentication

Especifica el método de autenticación de contraseña del nodo. Este parámetro es opcional.

Local

Especifica que desea bloquear los nodos que autentican las contraseñas con el servidor de IBM Spectrum Protect.

LDap

Especifica que desea desbloquear los nodos que autentican las contraseñas con el servidor de directorio LDAP.

Ejemplo: desbloquear un nodo

El nodo de cliente SMITH tiene bloqueado el acceso a IBM Spectrum Protect. Permitir que SMITH acceda al servidor.

```
unlock node smith
```

Ejemplo: Desbloquear todos los nodos que se autentican con el servidor de IBM Spectrum Protect

Los nodos que no autentican las contraseñas con servidores de directorio LDAP deben estar desbloqueado.

```
unlock node * authentication=local
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UNLOCK NODE

Mandato	Descripción
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.

UNLOCK PROFILE (Desbloquear un perfil)

Utilice este mandato en un gestor de configuración para desbloquear un perfil de configuración para que pueda distribuirse a los servidores gestionados que se inscriben.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UNLOCK PROFILE--nombre_perfil-----<<
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el perfil que se desbloquea. Puede utilizar caracteres comodín para especificar varios nombres.

Ejemplo: desbloquear un perfil

Desbloquear un perfil denominado TOM.

```
desbloquear el perfil tom
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UNLOCK PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UPDATE PROFILE	Cambia la descripción de un perfil.

Mandatos UPDATE

Utilice el mandato UPDATE para modificar uno o más atributos de un objeto IBM Spectrum Protect existente.

- UPDATE ADMIN (Actualizar un administrador)
- UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)
- UPDATE ALERTSTATUS (actualizar el estado de una alerta)
- UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)
- UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)

número_mensaje (Obligatorio)

Especifica el número de mensaje que desea asociar con el desencadenante de la alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres.

CATegory

Especifica el tipo de categoría de la alerta, que está determinado por los tipos de mensajes. El valor predeterminado es SERVER.

Nota: Si se cambia la categoría de un desencadenante de alerta, no se cambia la categoría de las alertas existentes en el servidor. Las nuevas alertas se clasifican dentro de la nueva categoría.

Especifique uno de los siguientes valores:

APplication

La alerta se clasifica como una categoría de aplicación. Por ejemplo, puede especificar esta categoría para los mensajes asociados con los clientes de aplicación (TDP).

INventory

La alerta se clasifica como categoría de inventario. Por ejemplo, puede especificar esta categoría para mensajes que están asociados con la base de datos, el archivo de registro activo o el archivo de registro de archivado.

CLient

La alerta se clasifica como una categoría de cliente. Por ejemplo, puede especificar esta categoría para los mensajes asociados con actividades de cliente generales.

DEvice

La alerta se clasifica como una categoría de dispositivo. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados a las clases de dispositivos, bibliotecas, unidades o vías de acceso.

SErver

La alerta se clasifica como una categoría de servidor general. Por ejemplo, puede especificar esta categoría para los mensajes asociados a las actividades del servidor generales o a sucesos.

STorage

La alerta se clasifica como una categoría de almacenamiento. Por ejemplo, puede especificar esta categoría para los mensajes asociados con las agrupaciones de almacenamiento.

SYstems

La alerta se clasifica como una categoría de clientes del sistema. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con los clientes de archivado y copia de seguridad del sistema o archivado y copia de seguridad de gestión de almacenamiento jerárquico (HSM).

VMclient

La alerta se clasifica bajo la categoría VMclient. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con clientes de máquina virtual.

ADmin

Este parámetro opcional especifica el nombre del administrador que recibe el correo electrónico de notificación de esta alerta. El desencadenante de alerta se ha definido satisfactoriamente aunque no se ha especificado ningún nombre de administrador.

ADDadmin

Especifica el nombre de administrador que desea agregar a la lista de administradores que reciben alertas por correo electrónico. Especifique varios nombres de administrador, separados por comas y sin espacios intercalados.

DELadmin

Especifica el nombre del administrador que desea suprimir de la lista de administradores que reciben alertas por correo electrónico. Especifique varios nombres de administrador, separados por comas y sin espacios intercalados.

Actualizar desencadenante de alerta

Añada los nombres de los administradores que desea que reciban la notificación cuando se produzca una alerta ANR1073E, ANR1074E, y suprima el nombre de un administrador que ya no desee que reciba la notificación, emitiendo el siguiente mandato:

```
update alerttrigger ANR1073E,ANR1074E ADDadmin=djee,cdawson,mhaye deladmin=harryh
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE ALERTTRIGGER

Mandato	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.

Mandato	Descripción
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

UPDATE ALERTSTATUS (actualizar el estado de una alerta)

Utilice este mandato para actualizar el estado de una alerta sobre la que se ha informado.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```

      .-,------.
      v          |
>>-UPDate ALERTStatus-----+--ID_alerta-+----->
>--+-----+-----+-----+----->
   '-SStatus-----+--Inactive-+-'   '-ASSigned-----texto-'
           '-Closed---'
>--+-----+-----+-----+-----><
   '-RESolvedby-----text-'   '-REMark-----text-'

```

Parámetros

id_alerta (Necesario)

Especifica la alerta que desea actualizar. Puede especificar varios números de mensaje separándolos con comas y sin espacios intercalados.

SStatus

Especifica el tipo de estado que desea actualizar. El estado de las alertas se puede cambiar a partir de activo a inactivo o cerrado, o de inactivo a cerrado. Los valores posibles son:

Inactivo

Las alertas activas pueden cambiar al estado inactivo.

Cerrado

Las alertas activas e inactivas pueden cambiar al estado cerrado.

ASSigned

Especifica el nombre del administrador que se asigna a la alerta que desea consultar.

RESolvedby

Especifica el nombre de administrador que ha resuelto la alerta que desea consultar.

REMark

Este parámetro especifica el texto de comentario. El texto de comentario no puede tener más de 255 caracteres. Si la descripción contiene espacios en blanco, escriba el texto entero entre comillas (""). Elimine el texto definido anteriormente especificando una serie nula ("") para este valor.

Actualizar el texto de comentario de una alerta

Emita el mandato siguiente para actualizar el texto de comentario y el número de ID de alerta 25 e indicar que DJADMIN está trabajando en la alerta:

```
update alertstatus 25 assigned=DJADMIN
```

Actualizar estado de alerta

Emita el mandato siguiente para cambiar el número de ID de alerta 72 al estado cerrado y agregar un comentario sobre cómo se ha resuelto la alerta:

```
update alertstatus 72 status=closed remark="Se ha aumentado el tamaño del sistema de
archivos para
el registro activo"
```



Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE ALERTSTATUS

Mandato	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.

UPDATE ADMIN (Actualizar un administrador)

Utilice este mandato para cambiar la contraseña o la información de contacto de un administrador. Sin embargo, no puede actualizar el nombre de administrador SERVER_CONSOLE.

 Sistemas operativos AIX  Sistemas operativos Linux Las contraseñas de los administradores deben cambiarse después de un periodo de tiempo que se determina mediante el mandato SET PASSEXP. El mandato SET PASSEXP no afecta a las contraseñas que se autentican con un servidor LDAP (Lightweight Directory Access Protocol).

Restricción: No puede actualizar el método de autenticación para su propio ID de usuario. Si es necesario, otro administrador debe hacer ese cambio. Asimismo, cuando actualiza una contraseña con el mandato UPDATE ADMIN, no puede utilizar un comodín con el parámetro `admin_name`.

Se pueden crear administradores con el mismo nombre como nodo durante un mandato REGISTER NODE . Para mantener el nodo y el administrador con el mismo nombre sincronizados, el método de autenticación y el valor de SSLREQUIRED del nodo se actualizan para coincidan con el del administrador. Si el método de autenticación de administrador se cambia de LOCAL a LDAP, y no se proporciona una contraseña, el nodo se coloca en estado "pendiente de LDAP". La contraseña se solicita en el siguiente inicio de sesión. Las contraseñas entre nodos y administradores con el mismo nombre se mantienen sincronizadas después de cualquier cambio de autenticación.

Debe utilizar el mandato RENAME ADMIN para cambiar el nombre de un administrador registrado.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Si un ID de usuario de administración coincide con un nombre de nodo, no actualice el método de autenticación a LDAP. Si lo hace, podría darse un comportamiento imprevisto, debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

Clase de privilegio

Para emitir este mandato para cambiar la contraseña o la información de contacto de otro administrador, debe tener privilegio de sistema. Cualquier administrador puede emitir este mandato para actualizar su propia contraseña o información de contacto.

Sintaxis

(1)

(2)

- En el caso de los ID de usuarios administrativos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si tiene previsto especificar AUTHENTICATION=LDAP.
- Si tiene previsto actualizar un ID de usuario administrativo para la autenticación con un servidor LDAP y ha especificado FORCEPWRESET=YES, debe cambiar la contraseña para poder especificar FORCEPWRESET=NO y AUTHENTICATION=LDAP.

EMAILAddress

Este parámetro se utiliza para información de contacto adicional. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

AUTHentication

Este parámetro determina el método de autenticación de la contraseña que utiliza el ID de administrador, bien LDAP o LOCAL.

Local

Especifica que el administrador utiliza la base de datos del servidor de IBM Spectrum Protect local para almacenar las contraseñas para la autenticación.

LDap

Especifica que el administrador utiliza un servidor de directorios LDAP para la autenticación de contraseñas.

SYNCLdapdelete

Este parámetro solo se aplica si un administrador que se autentica en un servidor LDAP quiere volver a la autenticación local.

Yes

Especifica que se ha de suprimir el administrador del servidor LDAP.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que no se ha de suprimir el administrador del servidor LDAP. Este es el valor predeterminado.

SSLrequired (en desuso)

Especifica si el ID de usuario administrador debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect y el cliente de archivado y copia de seguridad. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red.

Importante: A partir del software de IBM Spectrum Protect Versión 8.1.2 y del software de Tivoli Storage Manager Versión 7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

SESSIONSECurity

Especifica si el administrador debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el administrador. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el administrador. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el administrador pueda autenticarse en el servidor:

- Tanto el administrador como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el administrador para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el administrador.

Los administradores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

TRANSitional

Especifica que se aplicarán los valores de seguridad existentes para el administrador. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el administrador no cumplen nunca los requisitos para el valor STRICT, el administrador continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un administrador

cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el administrador ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el administrador se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un administrador que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como el direccionamiento de mandatos o la exportación entre servidores, cuando el administrador se autentica en el servidor IBM Spectrum Protect como administrador de otro servidor.

ALert

Especifica si las alertas se envían a una dirección de correo electrónico de los administradores.

Yes

Especifica que las alertas se envíen a la dirección de correo electrónico especificada de los administradores.

No

Especifica que las alertas no se envíen a la dirección de correo electrónico especificada de los administradores. Este es el valor predeterminado.

Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

Ejemplo: Actualizar una contraseña y el período de caducidad de la contraseña

Actualizar el administrador LARRY de modo que tenga la contraseña SECRETWORD y el período de caducidad de contraseña de 120 días. El administrador de este ejemplo se autentica en el servidor de IBM Spectrum Protect.

```
update admin larry secretword passexp=120
```

Ejemplo: Actualizar todos los administradores para comunicarse con un servidor utilizando la seguridad de sesión estricta.

Actualice todos los administradores para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
update admin * sessionsecurity=strict
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE ADMIN

Mandato	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

Tareas relacionadas:

Nombrar objetos de Tivoli Storage Manager

Referencia relacionada:

[Opción de cliente SSL](#)

UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)

Utilice este mandato para actualizar el valor de retención asociado al juego de copias de seguridad de un cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

Sintaxis

```
      .-,------.
      v          |
>>-UPDate BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'

      .-,------.
      v          |
>----nombre_juego_copias_seguridad+----->

>--RETention-----+días-----+----->
      '-NOLimit-'   '-BEGINDate-----fecha-'

>--+-----+-----+----->
      '-BEGINTime-----hora-'   '-ENDDate-----fecha-'

>--+-----+-----+----->
      '-ENDTime-----hora-'   '-WHERERETention-----+días-----+'
                                   '-NOLimit-'

      .-WHEREDATAType-----ALL-----
>--+-----+----->
      |          .-,------. |
      |          v          | |
      |'-WHEREDATAType-----+FILE--+-----'
      |          '-IMAGE-'

>--+-----+----->
      '-WHEREDEScRiption-----descripción-'

      .-VERSion-----Any-----
>--+-----+-----+-----><
      '-Preview-----No--+-'   '-VERSion-----+Any-----+'
      '-Yes-'                   '-Latest-'
```

Parámetros

nombre_nodo o nombre_grupo_nodos (Necesario)

Especifica los nombres de los nodos cliente o grupos de nodos cuyos datos se incluyen en el juego de copias de seguridad especificado que se ha de actualizar. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo que especifique pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener caracteres comodín.

nombre_juego_copias_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a actualizar. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

RETention (Obligatorio)

Especifica el número actualizado de días que se retiene el juego de copias de seguridad en el servidor. Puede especificar un entero entre el 0 y el 30000. Los valores son:

días

Especifica el número actualizado de días que se retiene el juego de copias de seguridad.

NOLimit

Especifica que el juego de copias de seguridad se retiene indefinidamente en el servidor. Si especifica NOLIMIT, el servidor retiene para siempre los volúmenes que contienen el juego de copias de seguridad, excepto si un usuario o un administrador suprime los volúmenes del almacenamiento del servidor.

Atención: la actualización del período de retención de un juego de copias de seguridad podría hacer que caducase a una hora diferente de otros juegos de copias de seguridad almacenados en el mismo medio de salida. En cualquier caso, el medio no estará disponible para otros usos hasta que todos sus juegos de copias de seguridad hayan caducado.

BEGINDate

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. El valor predeterminado es la fecha actual. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY-3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. El valor predeterminado es la hora actual. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-02:00 o -02:00.

ENDDate

Especifica la fecha final en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

ENDTime

Especifica la hora final en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

WHERERetention

Especifica, en días, el valor de retención asociado a los juegos de copias de seguridad que se van a actualizar. Los valores son:

días

Especifica que el juego de copias de seguridad que se va a retener el número de días especificado está actualizado.

NOLimit

Especifica que el juego de copias de seguridad retenido de forma indefinida está actualizado.

WHEREDescription

Especifica la descripción asociada al juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. Puede especificar caracteres comodín en la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

WHEREDataType

Especifica que se van a actualizar los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben actualizar. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben actualizar. Este es el valor predeterminado.

FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a actualizar. Los juegos de copias de seguridad de nivel de archivo contienen copias de seguridad de archivos y directorios realizadas por el cliente de copia de seguridad/archivado.

IMAGE

Especifica que se va a actualizar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad/archivado.

Preview

Especifica si se previsualiza la lista de los juegos de copias de seguridad que se van a actualizar, sin actualizar realmente los juegos de copias de seguridad. Este parámetro es opcional. El valor predeterminado es No. Los valores son:

No

Especifica que los juegos de copias de seguridad se actualizarán.

Yes

Especifica que el servidor visualiza la lista de los juegos de copias de seguridad que se van a actualizar, sin actualizarlos realmente.

VERSion

Especifica la versión del juego de copias de seguridad que se va a actualizar. Los juegos de copias de seguridad con el mismo nombre de prefijo se consideran versiones diferentes del mismo juego de copias de seguridad. Este parámetro es opcional. El valor predeterminado es actualizar cualquier versión que coincida con los criterios especificados en el mandato. Los valores son:

Any

Especifica que cualquier versión que coincida con los criterios especificados en el mandato debe actualizarse.

Latest

Especifica que únicamente debe actualizarse la versión más reciente del juego de copias de seguridad. Si otros criterios especificados en el mandato (por ejemplo, ENDDATE o WHERERETENTION) excluyen la versión más reciente del juego de copias de seguridad, no se actualizará ningún juego de copias de seguridad.

Ejemplo: actualizar un período de retención

Actualizar el periodo de retención donde la descripción es Healthy Computers. El periodo de retención se asigna al juego de copias de seguridad PERS_DATA.3099 que contiene datos del nodo cliente JANE. Cambiar el período de retención a 70 días.

```
update backupset jane pers_data.3099
retention=70 wheredescription="healthy computers"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE BACKUPSET

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)

Utilice este mandato para actualizar el número de secuencia de una opción de cliente en un conjunto de opciones de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-UPDate CLIENTOpt--nombre_conjunto_opciones--nombre_opción---->
>--número_secuencia_actual--número_secuencia_nueva-----<<
```

Parámetros

- nombre_conjunto_opciones (Obligatorio)
Especifica el nombre del conjunto de opciones.
- nombre_opción (Obligatorio)
Especifica una opción cliente válida.
- número_secuencia_actual (Obligatorio)
Especifica el número de secuencia actual de la opción.
- nuevo_número_secuencia (Obligatorio)
Especifica el nuevo número de secuencia de la opción.

Ejemplo: actualizar un número de secuencia de opción de cliente

Para actualizar el número de secuencia de la opción de cliente actual, emita el mandato siguiente:

```
update clientopt eng dateformat 0 9
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE CLIENTOPT

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.

UPDATE CLOPTSET (Actualizar la descripción de un conjunto de opciones de cliente)

Utilice este mandato para actualizar la descripción de un conjunto de opciones de cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

Sintaxis

```
>>-UPDate CLOptset--nombre_conjunto_opciones----->  
>--DESCRiption----descripción-----<
```

Parámetros

- nombre_conjunto_opciones (Obligatorio)
Especifica el nombre del conjunto de opciones.
- DESCRiption (Obligatorio)
Especifica una descripción del conjunto de opciones de cliente. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: actualizar la descripción de un conjunto de opciones de cliente

Actualizar la descripción de un conjunto de opciones de cliente denominado ENG.

```
update cloptset eng description="unix"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE CLOPTSET

Mandato	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.

UPDATE COLLOGROUP (Actualizar un grupo de proximidad)

Utilice este mandato para modificar la descripción de un grupo de proximidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate COLLOGGroup--nombre_grupo----->
>--DESCRiption--===descripción-----><
```

Parámetros

nombre_grupo

Especifica el nombre del grupo de proximidad cuya descripción desea actualizar.

DESCRiption (Obligatorio)

Especifica una descripción del grupo de proximidad. Este parámetro es necesario. La longitud máxima de la descripción es de 255 caracteres. Si la descripción contiene blancos, encierre toda la descripción entre comillas.

Ejemplo: actualizar un grupo de proximidad

Actualizar el grupo de proximidad, GROUP1, con una nueva descripción.

```
update colloggroup group1 "Human Resources"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE COLLOGROUP

Mandato	Descripción
DEFINE COLLOGGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.

Mandato	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

UPDATE COPYGROUP (Actualizar un grupo de copia)

Utilice este mandato para actualizar un grupo de copia de seguridad o de copia archivada. Para que los clientes puedan utilizar el grupo de copia actualizado, debe activar el juego de políticas que contiene el grupo de copia.

Consejo: El mandato UPDATE COPYGROUP no se ejecutará correctamente si especifica como destino una agrupación de almacenamiento de copia.

El mandato UPDATE COPYGROUP ofrece dos posibilidades, en función de si la actualización se realiza para un grupo de copias de seguridad o para un grupo de copias archivadas. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con UPDATE COPYGROUP

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.

- UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)
Utilice este mandato para actualizar un grupo de copia de seguridad definido.
- UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)
Utilice este mandato para actualizar un grupo de copia archivada definido.

UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)

Utilice este mandato para actualizar un grupo de copia de seguridad definido.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

Sintaxis

```

>>-UPDate COpYgroup----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+--+-----+----->
  '-STANDARD-' '-Type----Backup-'
>--+-----+--+-----+----->
  '-DEStination----nombre_agrupación-'
>--+-----+--+-----+----->
  '-FREQuency----días-' '-VERExists----+número--+-'
                                '-NOLimit-'
>--+-----+--+-----+----->
  '-VERDeleted----+número--+-'
                                '-NOLimit-'
>--+-----+--+-----+----->
  '-RETEExtra----+días--+-' '-RETOOnly----+días--+-'
                                '-NOLimit-'                                '-NOLimit-'
>--+-----+--+-----+----->
  '-MODE----+MODified+-'
                                '-ABSolute-'
>--+-----+--+-----+----->
  '-SERialization----+SHRStatic--+-'
                                +-Static-----+
                                +-SHRDYnamic+
                                '-DYnamic----'
>--+-----+--+-----+-----><
  '-TOCDestination----nombre_agrupación---'

```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el grupo de copia.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas al que pertenece el grupo de copia. No puede actualizar un grupo de copia del juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica la clase de gestión a la que pertenece el grupo de copia.

STANDARD

Especifica el grupo de copia, que debe ser STANDARD. Este parámetro es opcional.

Type=Backup

Especifica que desea actualizar un grupo de copia de seguridad. Este parámetro es opcional.

DEStination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los datos de copia de seguridad. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency

Especifica la frecuencia con la que el servidor puede hacer copia de seguridad de un archivo. Este parámetro es opcional. El servidor sólo hace copia de seguridad de un archivo cuando ha transcurrido el número de días especificado desde la última copia de seguridad. El valor de FREQUENCY sólo se utiliza durante una operación de copia de seguridad incremental. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial. Puede especificar un entero de 0 a 9999. El valor 0 significa que el servidor puede hacer copia de seguridad de un archivo independientemente del momento en que se hizo la última copia de seguridad del archivo.

VERExists

Especifica el número máximo de versiones de copia de seguridad para retener los archivos que actualmente se encuentran en el sistema de archivos del cliente. Este parámetro es opcional.

Si una copia de seguridad incremental hace que se sobrepase el límite, el servidor hará que caduque la versión de copia de seguridad más antigua que existe en el almacenamiento del servidor. Los valores posibles son:

número

Especifica el número de versiones de copia de seguridad a retener para los archivos que actualmente se encuentran en el sistema de archivos del cliente. Puede especificar un entero de 1 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 2. Los valores preferidos son 3, 4, o más.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad.

El número de versiones de copia de seguridad que se retienen se controla mediante este parámetro hasta que las versiones sobrepasen el tiempo de retención que especifica el parámetro RETEXTRA.

VERDeleted

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad utilizando el servidor. Este parámetro es opcional. Si un usuario suprime un archivo del sistema de archivos del cliente, la siguiente copia de seguridad incremental hará que el servidor cambie la versión de copia de seguridad activa del archivo a inactiva y que caduque las versiones más antiguas que sobrepasen este número. La fecha de caducidad de las versiones restantes se determina mediante el tiempo de retención especificado en los parámetros RETEXTRA y RETONLY. Los valores posibles son:

número

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad. Puede especificar un valor de 0 a 9999.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad de los archivos que se han suprimido del sistema de archivos del cliente después de hacerse la copia de seguridad.

RETEExtra

Especifica el número de días que servidor retiene una versión de copia de seguridad una vez que esa versión se convierte en inactiva. Una versión de un archivo se convierte en inactiva cuando el cliente almacena otra copia de seguridad más reciente o cuando el cliente suprime el archivo de la estación de trabajo y luego ejecuta una copia de seguridad incremental completa. El servidor suprime las versiones inactivas basándose en el tiempo de retención aunque el número de versiones inactivas no sobrepase el número que permiten los parámetros VEREXISTS o VERDELETED. Este parámetro es opcional. Los valores posibles son:

días

Especifica el número de días que se retienen las versiones de copia de seguridad inactivas. Puede especificar un entero de 0 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 14 días. El valor preferido es 30 días o más.

NOLimit

Especifica que las versiones de copia de seguridad inactivas se retienen de forma indefinida.

Si especifica NOLIMIT, el servidor suprime las versiones de copia de seguridad adicionales basándose en el parámetro VEREXISTS (si el archivo sigue existiendo en el sistema de archivos del cliente) o en el parámetro VERDELETED (si el archivo ya no existe en el sistema de archivos del cliente).

RETOOnly

Especifica el número de días que se retiene la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente. Este parámetro es opcional. Los valores posibles son:

días

Especifica el número de días que se han de retener la última copia de seguridad inactiva. Puede especificar un entero de 0 a 9999.

Consejo: Para asegurarse de que los archivos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 30 días.

NOLimit

Especifica que se desea conservar la última versión inactiva restante de un archivo de forma indefinida.

Si especifica NOLIMIT, el servidor retiene la última versión de copia de seguridad restante para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor.

MODE

Especifica si el servidor sólo hace copia de seguridad de un archivo si éste se ha modificado desde la última copia de seguridad o si la hace siempre que un cliente solicita una copia de seguridad. Este parámetro es opcional. Los valores posibles son:

MODified

Especifica que se realiza la copia de seguridad del archivo únicamente si se ha modificado desde la última copia de seguridad. Se considera que un archivo se ha modificado si se cumple algunas de las siguientes condiciones:

- La fecha de última modificación es diferente

- El tamaño del archivo es diferente
- El propietario del archivo es diferente
- Los permisos de los archivos son diferentes

ABSolute

Especifica que se realiza la copia de seguridad del archivo independientemente de si se ha modificado.

El valor de MODE sólo se utiliza en la copia de seguridad incremental completa. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial.

SERialization

Especifica cómo debe procesar el servidor los archivos o directorios cuando éstos se modifican durante el proceso de realización de la copia de seguridad. Este parámetro es opcional. Los valores posibles son:

SHRStatic

Especifica que el servidor sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. El servidor intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo o directorio se modifica durante cada intento de copia de seguridad, el servidor no hace la copia de seguridad.

STatic

Especifica que el servidor sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. El servidor intenta efectuar la copia de seguridad una sola vez.

Las plataformas que no admiten la opción STATIC establecen como valor predeterminado SHRSTATIC.

SHRDynamic

Especifica que si se modifica un archivo o directorio durante un intento de copia de seguridad, el servidor hace copia de seguridad del archivo o directorio durante el último intento aunque el archivo o directorio se esté modificando. El servidor intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

DYnamic

Especifica que el servidor realiza la copia de seguridad de un archivo o directorio en el primer intento, independientemente de que el archivo o directorio esté modificándose durante el proceso de copia de seguridad.

Importante: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar la copia de seguridad de un archivo o directorio mientras están produciéndose modificaciones. Como consecuencia, la versión de copia de seguridad puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se restaura un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una versión de copia de seguridad solo si el archivo o directorio no se está modificando.

TOCDestination

Especifica la agrupación de almacenamiento primaria en la que inicialmente se almacenará una tabla de contenido (TOC) para cualquier operación de copia de seguridad NDMP u operación de juego de copias de seguridad para la que se genere una TOC. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino. La agrupación de almacenamiento que se especifique para el destino debe tener el formato de datos NATIVE o NONBLOCK. Para evitar retrasos en el montaje, asegúrese de que la agrupación de almacenamiento tiene una clase de dispositivo DISK o DEVTYPE=FILE. La generación de la TOC es opcional en las operaciones de copia de seguridad NDMP, pero no está admitida en otras operaciones de copia de seguridad de imagen.

Para eliminar un destino de TOC existente del grupo de copias, especifique una serie nula ("") para este valor.

Si se solicita la creación de la TOC para una operación de copia de seguridad que utilice NDMP y la imagen está vinculada a una clase de gestión cuyo grupo de copia de seguridad no especifica un destino de TOC, el resultado de la operación dependerá del parámetro TOC de la operación de copia de seguridad.

- Si TOC=PREFERRED (el valor predeterminado), la copia de seguridad continuará sin crearse una TOC.
- Si TOC=YES, la copia de seguridad en su totalidad resultará anómala porque no puede crearse ninguna TOC.

Ejemplo: actualizar un grupo de copias de seguridad

Actualizar el grupo de copia de seguridad STANDARD del dominio de políticas EMPLOYEE_RECORDS, juego de políticas VACATION, clase de gestión ACTIVEFILES. El destino se cambiará a DISKPOOL, con un intervalo mínimo de siete días entre copias de seguridad, independientemente de si se han modificado los archivos. Se retendrán hasta tres versiones de copia de seguridad mientras exista un archivo en un sistema de archivos de cliente.

```
update copygroup employee_records vacation
activefiles type=backup destination=diskpool
frequency=7 verexists=3 mode=absolute
```

UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)

Utilice este mandato para actualizar un grupo de copia archivada definido.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

Sintaxis

```
>>-UPDate COpygroup----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+--Type---Archive----->
  '-STANDARD-'
>--+-----+----->
  '-DESTination---nombre_agrupación-'
>--+-----+----->
  '-FREQuency---Cmd-' '-RETVer---días--'
                                     '-NOLimit-'
>--+-----+----->
  '-MODE---ABSolute-' '-RETMin---días--'
>--+-----+-----<
  '-SERialization---+SHRStatic--+-'
                        +-STatic-----+
                        +-SHRDYnamic+
                        '-DYnamic----'
```

Parámetros

- nombre_dominio (Necesario)
Especifica el dominio de políticas al que pertenece el grupo de copia.
- nombre_juego_políticas (Necesario)
Especifica el juego de políticas al que pertenece el grupo de copia. No puede actualizar un grupo de copia del juego de políticas ACTIVE.
- nom_clase (Necesario)
Especifica la clase de gestión a la que pertenece el grupo de copia.
- STANDARD
Especifica el grupo de copias, que debe ser STANDARD. Este parámetro es opcional.
- Type=Archive (Necesario)
Especifica que desea actualizar un grupo de copia archivada. Este parámetro es necesario.
- DESTination
Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente la copia archivada. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino.
- FREQuency=Cmd
Especifica la frecuencia de copia, que debe ser CMD. Este parámetro es opcional.
- RETVer
Especifica el número de días que se ha de mantener una copia archivada. Este parámetro es opcional. Los valores posibles son:
 - días
Especifica el número de días que se ha de mantener una copia archivada. Puede especificar un entero entre el 0 y el 30000.
Consejo: Para asegurarse de que los datos pueden recuperarse tras un incidente malicioso, como por ejemplo un ataque de ransomware, especifique un valor de al menos 30 días.
- NOLimit
Especifica que desea conservar una copia archivada de forma indefinida.

Si especifica NOLIMIT, el servidor retendrá las copias archivadas sin límite de tiempo, a menos que un usuario o un administrador suprima el archivo del almacenamiento del servidor.

El valor del parámetro RETVER puede afectar a la clase de gestión a la que el servidor vincula un directorio de copia archivada. Si el cliente no utiliza la opción ARCHMC, el servidor vincula los directorios de copia archivada con la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor vincula los directorios de copia archivada con la clase de gestión que presente el período de retención más reducido.

MODE=ABSolute

Especifica que siempre se archiva un archivo cuando el cliente lo solicita. El valor de MODE debe ser ABSOLUTE. Este parámetro es opcional.

RETMIn

Especifica el número mínimo de días que se ha de mantener una copia archivada después de haberla archivado. Este parámetro es opcional. El valor predeterminado es 365.

SERialization

Especifica cómo debe procesar el servidor los archivos que se modifican durante la operación de archivado. Este parámetro es opcional. Los valores posibles son:

SHRStatic

Especifica que el servidor no guarda una copia archivada de un archivo que se está modificando. El servidor intenta efectuar una operación de archivado cuatro veces como máximo, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo se modifica durante el intento de archivado, el servidor no archivará el archivo.

Static

Especifica que el servidor no guarda una copia archivada de un archivo que se está modificando. Si un archivo se modifica durante el intento de archivado, el servidor no archivará el archivo.

Las plataformas que no admiten la opción STATIC establecen como valor predeterminado SHRSTATIC.

SHRDynamic

Especifica que si se modifica el archivo durante un intento de archivar, el servidor archivará el archivo en el último intento aunque se esté modificando. El servidor intenta la operación de archivado cuatro veces como máximo, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

Dynamic

Especifica que el servidor realiza la copia archivada de un archivo en el primer intento, independientemente de si el archivo está modificándose durante el proceso de archivado.

Importante: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar una operación de archivado de un archivo mientras están produciéndose modificaciones. Como consecuencia, la copia archivada puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se recupera un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una copia de archivado solo si el archivo no se está modificando.

Consejo: Proceda con precaución al seleccionar valores de retención para agrupaciones de almacenamiento primarias con el tipo CLAMATIONTYPE=SNAPLOCK. Los volúmenes con este tipo de agrupación de almacenamiento no se pueden suprimir hasta que no han sobrepasado sus fechas de retención.

Ejemplo: actualizar varios elementos de un grupo de copias

Actualizar el grupo de copia archivada STANDARD del dominio de políticas EMPLOYEE_RECORDS, juego de políticas VACATION, clase de gestión ACTIVEFILES. Se cambiará el destino a TAPEPOOL. Las copias archivadas se conservarán 190 días.

```
update copygroup employee_records vacation
activefiles standard type=archive
destination=tapepool retver=190
```

UPDATE DATAMOVER (Actualizar un transportador de datos)

Utilice este mandato para actualizar la definición de un transportador de datos o para poner fuera de línea un transportador de datos cuando se somete a mantenimiento el hardware.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DATAMover--nombre_transportador_datos----->
>+-----+-----+-----+-----+-----+-----+----->
  '-HLAddress----dirección-'  '-LLAddress----puerto_tcp-'
>+-----+-----+-----+-----+-----+-----+----->
  '-USERid----ID_usuario-'  '-PASsword----contraseña-'
>+-----+-----+-----+-----+-----+-----+-----><
  '-ONLine----+Yes-+-'
                    '-No--'
```

Parámetros

nombre_transportador_datos (Obligatorio)

Especifica el nombre del transportador de datos.

HLAddress

Especifica la nueva dirección IP numérica o el nuevo nombre de dominio, que se utiliza para acceder al servidor de archivos NAS. Este parámetro es opcional.

LLAddress

Especifica el nuevo número de puerto TCP para acceder al servidor de archivos NAS para sesiones con el protocolo NDMP (Network Data Management Protocol). Este parámetro es opcional.

USERid

Especifica el ID de un usuario autorizado para iniciar una sesión con el servidor de archivos NAS. Por ejemplo, especifique el ID de administración de un servidor de archivos NetApp. Este parámetro es opcional.

PASsword

Especifica la nueva contraseña del ID de usuario para iniciar una sesión en el servidor de archivos NAS. Este parámetro es opcional.

ONLine

Especifica si el transportador de datos está disponible para utilizarlo. Este parámetro es opcional.

Yes

Especifica que el transportador de datos está disponible para utilizarlo.

No

Especifica que el transportador de datos no está disponible para utilizarlo.

Atención: Si se controla una biblioteca mediante una ruta desde un transportador de datos a la biblioteca y el transportador de datos está desactivado, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras el transportador de datos está desactivado, no se inicializará la biblioteca.

Ejemplo: actualizar la dirección IP de un transportador de datos

Actualizar el transportador de datos para el nodo denominado NAS1. Cambiar la dirección IP numérica 9.67.97.103 por 9.67.97.109.

```
update datamover nas1 hladdress=9.67.97.109
```

Ejemplo: actualizar el nombre de dominio de un transportador de datos

Actualizar el transportador de datos para el nodo denominado NAS1. Cambiar la dirección IP numérica 9.67.97.109 por el nombre de dominio NETAPP2.TUCSON.IBM.COM.

```
update datamover nas1 hladdress=netapp2.tucson.ibm.com
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE DATAMOVER

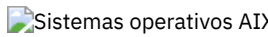
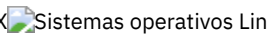
Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DATAMOVER	Suprimir un transportador de datos.

Mandato	Descripción
QUERY DATAMOVER	Visualiza definiciones de transportador de datos.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

UPDATE DEVCLASS (Actualizar los atributos de una clase de dispositivo)

Utilice este mandato para actualizar una clase de dispositivo definida.

Nota: La clase de dispositivo DISK viene predefinida por IBM Spectrum Protect y no puede modificarse con el mandato UPDATE DEVCLASS.

 Sistemas operativos AIX  Sistemas operativos Linux Si está actualizando una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS).

La sintaxis y las descripciones de los parámetros se proporcionan según el tipo de dispositivo. La información de sintaxis y parámetros se presenta en el orden siguiente.

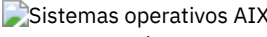
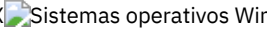
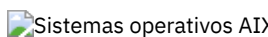
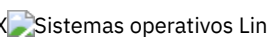
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 4MM)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 8MM)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo CENTERA)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo DLT)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE)
-  Sistemas operativos AIX  Sistemas operativos Windows UPDATE DEVCLASS (Actualizar una clase de dispositivo GENERICTAPE)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo LTO)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo NAS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo REMOVABLEFILE)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo SERVER)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo VOLSAFE)

Tabla 1. Mandatos relacionados con UPDATE DEVCLASS

Mandato	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590)

Utilice la clase de dispositivo 3590 cuando utilice dispositivos de cinta 3590.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

```

>>-UPDate DEVclass--nombre_clase_dispositivo----->
>+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>+-----+-----+----->
  '-FORMAT-----DRIVE---'  '-ESTCAPacity----tamaño-'
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'
>+-----+-----+----->
  '-PREFIX-----ADSM-----+'
      '-prefijo_volumen_cinta-'
>+-----+-----+----->
  '-MOUNTRetention----minutos-'  '-MOUNTWait----minutos-'
>+-----+-----+-----><
  '-MOUNTLimit-----DRIVES--+'
      +-número-+
      '-0-----'

```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En las tablas siguientes se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3590:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para 3590

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3590B	10 GB	Formato sin comprimir (básico)
3590C	Consulte la nota 20 GB	Formato comprimido
3590E-B	10 GB	Formato sin comprimir (básico), similar al formato 3590B

Formato	Capacidad estimada	Descripción
3590E-C	Consulte la nota 20 GB	Formato comprimido, similar al formato 3590C
3590H-B	30 GB (cartucho J, longitud estándar) 60 GB (cartucho K, longitud ampliada)	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Consulte la nota 60 GB (cartucho J, longitud estándar) 120 GB (cartucho K, longitud ampliada)	Formato comprimido, similar al formato 3590C

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

Tabla 2. Selecciones de formato de grabación de dispositivos 3590

Dispositivo	Formato					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Lectura/	Lectura/	–	–	–	–
Ultra-SCSI	Grabación	Grabación	–	–	–	–
3590E	Lectura/	Lectura/	Lectura/	Lectura/	–	–
3590H	Grabación	Grabación	Grabación	Grabación	Lectura/	Lectura/
	Lectura	Lectura	Lectura	Lectura	Grabación	Grabación
	Lectura	Lectura				

ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.



número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592)

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRary---nombre_biblioteca-'
>--+-----+----->
  '-LBProtect---+READWrite+-'
```



```

+-WRITEOnly+
'-No-----'

>----->
'-SCALECAPacity---+100--+-' '-FORMAT---+DRIVE---+-'
          +-90--+          +-3592-----+
          '-20--'          +-3592C----+
                          +-3592-2---+
                          +-3592-2C--+
                          +-3592-3---+
                          +-3592-3C--+
                          +-3592-4---+
                          +-3592-4C--+
                          +-3592-5---+
                          +-3592-5C--+
                          +-3592-5A--+
                          '-3592-5AC-'

>----->
'-ESTCAPacity---+tamaño-'

>----->
'-PREFIX---+ADSM-----+'
          '-prefijo_volumen_cinta-'

>----->
'-MOUNTRetention---+minutos-' '-MOUNTWait---+minutos-'

>----->
'-MOUNTLimit---+DRIVES--+-'
          +-número--+
          '-0-----'

>-----<
| (1) (2) |
|-----DRIVEEncryption---+ON-----|
          +-ALLOW----+
          +-EXTERNAL--+
          '-OFF-----'

```

Notas:

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. Se admite el cifrado de unidad solo para la segunda generación de unidades 3592 o posteriores.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

READWRITE

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de

cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades IBM® 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.

Consulte la nota técnica 1634851, Información adicional sobre la opción LBProtect de Tivoli Storage Manager, para ver una explicación sobre cuándo utilizar el parámetro LBProtect.

SCALECapacity

Especifica el porcentaje de la capacidad del medio que puede utilizarse para almacenar datos. Este parámetro es opcional. Los valores posibles son 20, 90 y 100.

Si se establece en 100 el porcentaje de la capacidad de escala, se proporciona la capacidad máxima de almacenamiento. Si se establece en 20 se obtiene el tiempo de acceso más rápido.

Nota: El valor de la capacidad de escala entra en vigor cuando se graban datos por primera vez en un volumen. Cualquier actualización de la clase de dispositivo de capacidad de escala no afecta a los volúmenes que ya tienen datos grabados hasta que el volumen se vuelve a poner en estado reutilizable.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3592.

Consejo: El nombre de formato se especifica como, por ejemplo, 3592-X, 3592-XC, 3592-XA, o 3592-XAC, donde X indica la generación de la unidad, C indica un formato comprimido, y A indica una unidad de archivado.

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para 3592

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3592	300 GB	Formato sin comprimir (básico)
3592C	Consulte la nota.	Formato comprimido
3592-2	500 GB	Cintas JA con formato sin comprimir (básico)
	700 GB	Cintas JB con formato sin comprimir (básico)
3592-2C	1,5 TB	Cintas JA con formato comprimido
	2,1 TB	Cintas JB con formato comprimido

Formato	Capacidad estimada	Descripción
3592-3	640 GB	Cintas JA con formato sin comprimir (básico)
	1 TB	Cintas JB con formato sin comprimir (básico)
3592-3C	1,9 TB	Cintas JA con formato comprimido
	3 TB	Cintas JB con formato comprimido
3592-4	400 GB	Cintas JB con formato sin comprimir (básico)
	1,5 TB	Cintas JB con formato sin comprimir (básico)
	3,1 TB	Cintas JC con formato sin comprimir (básico)
3592-4C	1,2 TB	Cintas JK con formato comprimido
	4,4 TB	Cintas JB con formato comprimido
	9,4 TB	Cintas JC con formato comprimido
3592-5 (Para unidades IBM TS1150 Modelo 3592 E08 con ID de producto 03592E08)	900 GB	Cintas JB con formato sin comprimir (básico)
	7000 GB	Cintas JC/JY con formato sin comprimir (básico)
	2000 GB	Cintas JL con formato sin comprimir (básico)
	10.000 GB	Cintas JD/JZ con formato sin comprimir (básico)
3592-5C (Para unidades IBM TS1150 Modelo 3592 E08 con ID de producto 03592E08)	Depende de la compresibilidad de datos	Cintas JK con formato comprimido
		Cintas JC/JY con formato comprimido
		Cintas JL con formato comprimido
		Cintas JD/JZ con formato comprimido
3592-5A (Para unidades IBM TS1155 Modelo 3592 55F con ID de producto 0359255F)	3.000 GB	Cintas JL con formato sin comprimir (básico)
	15.000 GB	Cintas JD/JZ con formato sin comprimir (básico)
3592-5AC (Para unidades IBM TS1155 Modelo 3592 55F con ID de producto 0359255F)	Depende de la compresibilidad de datos	Cintas JL con formato comprimido
		Cintas JD/JZ con formato comprimido
Nota: Si este formato utiliza la función de compresión de unidades de cintas, en función de la eficacia de la compresión, la capacidad real podría ser distinta a la capacidad estimada.		

Importante: Para un rendimiento óptimo, evite combinar distintas generaciones de unidades en una única biblioteca SCSI.

También se necesitan configuraciones especiales para combinar distintas generaciones de unidades 3592 en bibliotecas 349x y ACSLS.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:
`AB.CD2.E`
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 4 mm que ha utilizado esta clase de dispositivo. Este parámetro es opcional. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 4 mm:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para las cintas de 4 mm

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DDS1	1,3 GB (60 metros) 2,0 GB (90 metros)	Formato sin comprimir, sólo aplicable a cintas de 60 y 90 metros
DDS1C	Consulte la nota 1,3 GB (60 metros) 2,0 GB (90 metros)	Formato comprimido, sólo aplicable a cintas de 60 y 90 metros
DDS2	4 GB	Formato sin comprimir, sólo se aplica a cintas de 120 metros
DDS2C	Consulte la nota 8 GB	Formato comprimido, sólo se aplica a cintas de 120 metros
DDS3	12 GB	Formato sin comprimir, sólo se aplica a cintas de 125 metros
DDS3C	Consulte la nota 24 GB	Formato comprimido, sólo se aplica a cintas de 125 metros
DDS4	20 GB	Formato sin comprimir, sólo se aplica a cintas de 150 metros
DDS4C	Consulte la nota 40 GB	Formato comprimido, sólo se aplica a cintas de 150 metros
DDS5	36 GB	Formato sin comprimir cuando se utilizan medios DAT 72
DDS5C	Consulte la nota 72 GB	Formato comprimido cuando se utilizan medios DAT 72
DDS6	80 GB	Formato sin comprimir, cuando se utilizan medios DAT 160
DDS6C	Consulte la nota 160 GB	Formato comprimido, cuando se utilizan medios DAT 160

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 4 mm, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del nombre de archivo en el que el servidor graba las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

UPDATE DEVCLASS (Actualizar una clase de dispositivo 8MM)

Utilice la clase de dispositivo 8MM cuando utilice dispositivos de cinta de 8 mm.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-FORMAT----+DRIVE--'  '-ESTCAPacity----tamaño-'
      +-8200--+
      +-8200C--+
      +-8500--+
      +-8500C--+
      +-8900--+
      +-AIT----+
      +-AITC--+
      +-M2-----+
      +-M2C---+
      +-SAIT--+
      +-SAITC--+
      +-VXA2--+
      +-VXA2C--+
      +-VXA3--+
      '-VXA3C-'
>--+-----+----->
  '-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'
>--+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>--+-----+-----<
  '-MOUNTLimit----+DRIVES--'
      +-número+
      '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 8 mm que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 8 mm:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para cintas de 8 mm

Formato Tipo de medio	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
8200	2,3 GB	Formato sin comprimir (estándar) con cartuchos de cintas de 112 metros
8200C	Consulte la nota 3,5 GB 4,6 GB	Formato comprimido con cartuchos de cintas de 112 metros estándar
8500 15 m 15 m 15 m 54 m 54 m 54 m 112 m 112 m 112 m 160 m XL	Consulte la nota 600 MB 600 MB 600 MB 2,35 GB 2,35 GB 2,35 GB 5 GB o 10 GB 5 GB o 10 GB 5 GB o 10 GB 7 GB	Unidades (Lectura Grabación) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW)
8500C 15 m 15 m 15 m 54 m 54 m 54 m 112 m 112 m 112 m 160 m XL	Consulte la nota 1,2 GB 1,2 GB 1,2 GB 4,7 GB 4,7 GB 4,7 GB 5 GB o 10 GB 5 GB o 10 GB 5 GB o 10 GB 7 GB	Unidades (Lectura Grabación) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW)

Formato		Descripción
Tipo de medio	Capacidad estimada	
8900	Consulte la nota	Unidad (Lectura Grabación)
15 m	–	Mammoth 8900 (R)
54 m	–	Mammoth 8900 (R)
112 m	–	Mammoth 8900 (R)
160 m XL	–	Mammoth 8900 (R)
22 m	2,5 GB	Mammoth 8900 (RW)
125 m	–	Mammoth 8900 (RW con actualización)
170 m	40 GB	Mammoth 8900 (RW)
AIT	Consulte la nota	Unidad
SDX1–25C	25 GB	Unidades
SDX1–35C	35 GB	AIT, AIT2 y AIT3
SDX2–36C	36 GB	Unidades
SDX2–50C	50 GB	AIT, AIT2 y AIT3
SDX3–100C	100 GB	Unidades AIT2 y AIT3
SDX3X-150C	150 GB	Unidades AIT2 y AIT3
SDX4–200C	200 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	400 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5
AITC	Consulte la nota	Unidad
SDX1–25C	50 GB	Unidades
SDX1–35C	91 GB	AIT, AIT2 y AIT3
SDX2–36C	72 GB	Unidades
SDX2–50C	130 GB	AIT, AIT2 y AIT3
SDX3–100C	260 GB	Unidades AIT2 y AIT3
SDX3X-150C	390 GB	Unidades AIT2 y AIT3
SDX4–200C	520 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	1040 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5
M2	Consulte la nota	Unidad (Lectura Grabación)
75 m	20 GB	Mammoth II (RW)
150 m	40 GB	Mammoth II (RW)
225 m	60 GB	Mammoth II (RW)
M2C	Consulte la nota	Unidad (Lectura Grabación)
75 m	50 GB	Mammoth II (RW)
150 m	100 GB	Mammoth II (RW)
225 m	150 GB	Mammoth II (RW)
SAIT	Consulte la nota	Unidad (Lectura Grabación)
	500 GB	Sony SAIT1–500(RW)
SAITC	Consulte la nota	Unidad (Lectura Grabación)
	1300 GB (1,3 TB)	Sony SAIT1–500(RW)
VXA2	Consulte la nota	Unidad (Lectura Grabación)
V6 (62 m)	20 GB	VXA–2
V10 (124 m)	40 GB	
V17 (170 m)	60 GB	

Formato		Descripción
Tipo de medio	Capacidad estimada	
VXA2C V6 (62 m) V10 (124 m) V17 (170 m)	Consulte la nota 40 GB 80 GB 120 GB	Unidad (Lectura Grabación) VXA-2
VXA3 X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 40 GB 86 GB 160 GB	Unidad (Lectura Grabación) VXA-3
VXA3C X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 80 GB 172 GB 320 GB	Unidad (Lectura Grabación) VXA-3
<p>Nota: Las capacidades reales pueden variar en función de los cartuchos y las unidades que se utilicen.</p> <ul style="list-style-type: none"> • Para los formatos AITC y SAITC, la proporción de compresión normal es de 2.6:1. • Para el formato M2C, la proporción de compresión normal es de 2,5:1. 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 8 mm, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

Ejemplo: actualizar el límite de montaje y la capacidad de una clase de dispositivo de 8 mm

Actualizar una clase de dispositivo denominada 8MMTAPE. Cambiar el límite de montaje por 3 y la capacidad estimada por 10 GB.

```
update devclass 8mmtape mountlimit=3 estcapacity=10G
```

Ejemplo: actualizar el período de retención de montaje de una clase de dispositivo de 8 mm

Actualizar una clase de dispositivo de 8 mm que se denomina 8MMTAPE en una retención de montaje de 15 minutos.

```
update devclass 8mmtape mountretention=15
```

UPDATE DEVCLASS (Actualizar una clase de dispositivo CENTERA)

Utilice la clase de dispositivo CENTERA cuando utilice dispositivos de almacenamiento EMC Centera. El tipo de dispositivo CENTERA utiliza los archivos como volúmenes para almacenar los datos de forma secuencial. Es similar a la clase de dispositivo FILE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```

>>-UPDate DEVclass--nombre_clase_dispositivo----->
                                     (1)
>--HLAddress-----dirección_ip?archivo_PEA----->
>+-----+-----+-----+-----+-----+----->
  '-MINCAPacity-----tamaño---'
>+-----+-----+-----+-----+-----+-----><
  '-MOUNTLimit-----número---'

```

Notas:

1. Para cada clase de dispositivo Centera, debe especificar una dirección IP. Sin embargo, la ruta y el nombre del archivo PEA (autorización de entrada de agrupación) son opcionales, y la especificación del archivo PEA debe indicarse después de la dirección IP. Utilice el carácter "?" para separar la ruta y el nombre de archivo PEA de la dirección IP.

Parámetros


nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.


HLAddress

Especifica una dirección IP para el dispositivo de almacenamiento Centera y, opcionalmente, el nombre y la ruta de un archivo PEA (autorización de entrada de agrupación). Especifique las direcciones IP en formato decimal con punto (por ejemplo, 9.10.111.222). Un dispositivo Centera puede tener varias direcciones IP. Sin embargo, solo es necesario especificar una como valor para este parámetro.

 Sistemas operativos AIX La ruta y el nombre del archivo PEA son sensibles a las mayúsculas y minúsculas.

Si agrega el nombre y la ruta de un archivo PEA, asegúrese de que el archivo se almacena en un directorio del sistema que ejecuta el servidor de IBM Spectrum Protect. Separe el nombre y la ruta del archivo PEA de la dirección o direcciones IP con "?" como por ejemplo:  Sistemas operativos Windows

```
HLADDRESS=9.10.111.222?c:\controlFiles\TSM.PEA
```

 Sistemas operativos AIX

```
HLADDRESS=9.10.111.222?/user/ControlFiles/TSM.PEA
```

Especifique sólo una ruta y nombre de archivo PEA para cada definición de clase de dispositivo. Si especifica dos clases de dispositivo Centera distintas que hagan referencia al mismo dispositivo de almacenamiento Centera y si las definiciones de clase de dispositivo contienen distintas rutas y nombres de archivo PEA, el servidor utiliza el archivo PEA especificado en el parámetro HLADDRESS de la clase de dispositivo que se haya utilizado en primer lugar para abrir el dispositivo de almacenamiento Centera.

Nota:

1. El servidor no incluye un archivo PEA durante la instalación. Si no crea ningún archivo PEA, el servidor utilizará el perfil predeterminado de Centera, que permite a las aplicaciones leer, escribir, suprimir, depurar y consultar datos de un dispositivo de almacenamiento Centera. Para conseguir un control más estricto, cree un archivo PEA utilizando la interfaz de línea de mandatos proporcionada por EMC Centera. Para obtener detalles sobre la autenticación y autorización de Centera, consulte la publicación *Programmer's Guide* de EMC Centera.
2. También puede especificar la ruta y el nombre del archivo PEA en una variable de entorno utilizando la sintaxis CENTERA_PEA_LOCATION=rutaarchivo_nombearchivo. La ruta y el nombre del archivo PEA especificados en esta variable de entorno se aplicarán a todos los clústeres de Centera. Si utiliza esta variable, no es necesario que especifique la ruta y el nombre del archivo PEA utilizando el parámetro HLADDRESS.
3. Al actualizar la clase de dispositivo con un nombre y ubicación del archivo PEA nuevos o cambiados, es posible que se requiera reiniciar el servidor si ya se ha accedido al dispositivo Centera identificado por la dirección IP en la instancia actual del servidor.

MINCAPacity

Especifica el nuevo tamaño mínimo para los volúmenes Centera que se asignan a una agrupación de almacenamiento de esta clase de dispositivo. Este valor representa la cantidad mínima de datos que se almacenan en un volumen Centera antes de que el servidor lo marque como lleno. Los volúmenes Centera seguirán aceptando datos hasta que se haya almacenado la cantidad mínima de datos. Este parámetro es opcional.

tamaño

Especifique este valor como un entero seguido de **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor mínimo permitido es 1 MB (MINCAPACITY=1M). El valor máximo permitido es 128 GB (MINCAPacity=128G).

MOUNTLimit

Especifica el número máximo nuevo de sesiones que acceden al dispositivo Centera. Este parámetro es opcional. Puede especificar un número a partir de 0 o mayor; no obstante, la suma de todos los valores de límite de montaje para todas las clases de dispositivo asignadas al mismo dispositivo Centera no debe superar el número máximo de sesiones que permite Centera.

UPDATE DEVCLASS (Actualizar una clase de dispositivo DLT)

Utilice la clase de dispositivo DLT cuando utilice dispositivos de cinta DLT.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>+-----+----->
  '-FORMAT----+DRIVE---+'  '-ESTCAPacity---tamaño-'
      +-DLT1-----+
      +-DLT1C----+
      +-DLT10----+
      +-DLT10C---+
      +-DLT15----+
      +-DLT15C---+
      +-DLT20----+
      +-DLT20C---+
      +-DLT35----+
      +-DLT35C---+
      +-DLT40----+
      +-DLT40C---+
      +-DLT2-----+
      +-DLT2C----+
      +-DLT4-----+
      +-DLT4C----+
      +-SDLT-----+
      +-SDLTC----+
      +-SDLT320--+
      +-SDLT320C-+
      +-SDLT600--+
      +-SDLT600C-+
      +-DLTS4----+
      '-DLTS4C---'
>+-----+----->
  '-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'
>+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>+-----+-----<
  '-MOUNTLimit---+DRIVES--+'
      +-numero+
      '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas DLT que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos DLT:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para DLT

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DLT1	40 GB	Formato sin comprimir sólo con cartuchos CompacTape III o CompacTape IV
DLT1C	Consulte la nota 1. 80 GB	Formato comprimido sólo con cartuchos CompacTape III y CompacTape IV
DLT10	10 GB	Formato sin comprimir sólo con cartuchos CompacTape III o CompacTape IV
DLT10C	Consulte la nota 1. 20 GB	Formato comprimido sólo con cartuchos CompacTape III y CompacTape IV
DLT15	15 GB	Formato sin comprimir sólo con cartuchos CompacTape IIIxt o CompacTape IV (no CompacTape III) Nota: Válido con unidades DLT2000XT, DLT4000 y DLT7000
DLT15C	Consulte la nota 1. 30 GB	Formato comprimido sólo con cartuchos CompacTape IIIxt o CompacTape IV (no CompacTape III) Válido con unidades DLT2000XT, DLT4000 y DLT7000
DLT20	20 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20C	Consulte la nota 1. 40 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT35	35 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT35C	Consulte la nota 1. 70 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT40	40 GB	Formato sin comprimir sólo con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT40C	Consulte la nota 1. 80 GB	Formato comprimido con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT2	80 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLTtape VS1
DLT2C	Consulte la nota 1. 160 GB	Formato comprimido, cuando se utilizan medios Quantum DLTtape VS1
DLT4	160 GB	Formato sin comprimir, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4

Formato	Capacidad estimada	Descripción
DLT4C	Consulte la nota 1. 320 GB	Formato comprimido, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
SDLT Consulte la nota 2.	100 GB	Formato sin comprimir con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLTC Consulte la nota 2.	Consulte la nota 1. 200 GB	Formato comprimido con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLT320 Consulte la nota 2.	160 GB	Formato sin comprimir, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT320C Consulte la nota 2.	Consulte la nota 1. 320 GB	Formato comprimido, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT600	300 GB	Formato sin comprimir, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT
SDLT600C	Consulte la nota 1. 600 GB	Formato comprimido, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT
DLTS4	800 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4
DLTS4C	Consulte la nota 1. 1,6 TB	Formato comprimido, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4
<p>Nota:</p> <ol style="list-style-type: none"> 1. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista. 2. IBM Spectrum Protect no admite una biblioteca que contenga unidades SDLT BRC (Backward Read Compatible) y SDLT NBRC (Non-Backward Read Compatible). 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información sobre capacidades estimadas, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número



Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE)

Utilice la clase de dispositivo ECARTRIDGE cuando está utilizando unidades StorageTek tales como StorageTek T10000 o T9840.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-LBProtect---+READWrite+-'
                    +-WRITEOnly-+
                    '-No-----'
>--+-----+-----+----->
  '-FORMAT-----+DRIVE-----+'  '-ESTCAPacity----tamaño-'
                    +-T9840C----+
                    +-T9840C-C--+
                    +-T9840D----+
                    +-T9840D-C--+
                    +-T10000A---+
                    +-T10000A-C-+
                    +-T10000B---+
                    +-T10000B-C-+
                    +-T10000C---+
                    +-T10000C-C-+
                    +-T10000D---+
                    '-T10000D-C-'
>--+-----+-----+----->
  '-PREFIX-----+ADSM-----+'
                    '-prefijo_volumen_cinta-'
>--+-----+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>--+-----+-----+----->
  '-MOUNTLimit-----+DRIVES-+-'
                    +-número-+
                    '-0-----'
>--+-----+-----+-----><
  | (1) (2) |
  '-----DRIVEEncryption-----+ON-----+'
                    +-ALLOW----+
                    +-EXTERNAL-+
                    '-OFF-----'
```

Notas:

1. Puede utilizar el cifrado de unidad solo en unidades Oracle StorageTek T10000B con un valor de formato de DRIVE, T10000B o T10000B-C, para unidades Oracle StorageTek T10000C con un valor de formato de DRIVE, T10000C o T10000C-C y para unidades Oracle StorageTek T10000D con un valor de formato de DRIVE, T10000D y T10000D-C.
2. No puede especificar WORM=YES y DRIVEENCRYPTION=ON a la vez.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido con las unidades de cintas ECARTRIDGE que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades Oracle StorageTek T10000C y Oracle StorageTek T10000D.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

Importante: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos ECARTRIDGE:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000

Formato	Capacidad estimada	Descripción
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Notas:</p> <ul style="list-style-type: none"> Algunos formatos utilizan la función de compresión por hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista. Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C. 		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:
AB.CD2.E
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de

dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional.

Restricción:

1. Solo puede utilizar el cifrado de unidad en las siguientes unidades:
 - Las unidades Sun StorageTek T10000B con un valor de formato DRIVE, T10000B o T10000B-C
 - Las unidades Sun StorageTek T10000C con un valor de formato DRIVE, T10000C o T10000C-C
 - Unidades Oracle StorageTek T10000D con un valor de formato DRIVE, T10000D o T10000D-C
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=YES y DRIVEENCRYPTION=ON a la vez).
3. Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM



Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.


OFF



Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE)

Utilice la clase de dispositivo FILE si utiliza archivos en el almacenamiento de disco magnético como volúmenes que almacenan datos secuencialmente (como en una cinta).

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS).

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+-----+-----+----->
  '-MOUNTLimit-----número-'  '-MAXCAPacity-----tamaño-'
>--+-----+-----+-----+-----+----->
  |                               .-,-----|. |
  |                               v          | |
  '-DIRectory-----nombre_directorio-+-'
>--+-----+-----+-----+-----+-----><
  '-SHARED-----+No--+-'
  '-Yes--'
```


Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

 Sistemas operativos Windows Si desea compartir la clase de dispositivo con un agente de almacenamiento (mediante la especificación del parámetro SHARED=YES), se definirán o se suprimirán unidades en función del valor de MOUNTLIMIT.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

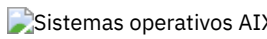
MAXCAPacity

Especifica el tamaño máximo de los archivos de almacenamiento de datos clasificados por esta clase de dispositivo. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). Si está definiendo una clase de dispositivo FILE para los volúmenes de copia de seguridad de base de datos, especifique un valor para MAXCAPACITY que sea adecuado para el tamaño de la base de datos y que minimice el número de volúmenes de base de datos.

Por ejemplo, MAXCAPACITY=5G especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 gigabytes. El valor especificado debe ser menor o igual que el tamaño máximo admitido de un archivo en el sistema de archivos

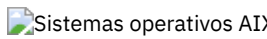
destino.

 Sistemas operativos AIX/Sistemas operativos Linux No defina un valor para MAXCAPACITY superior a 640M cuando este archivo se destine al soporte de CD REMOVABLEFILE. Un valor menor que un espacio utilizable del CD (650 MB) permite una coincidencia unívoca entre los archivos de la clase de dispositivo FILE y las copias que se encuentran en el CD.

DIRectory

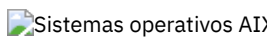
Especifica las ubicaciones del directorio de los archivos utilizados en esta clase de dispositivo. Escriba comillas al principio y al final de la lista de directorios y utilice comas para separar los nombres de directorio individuales. Se permiten los caracteres especiales (por ejemplo, espacios en blanco) en los nombres de directorio. Por ejemplo, la lista de directorios "abc def,xyz" contiene dos directorios: abc def y xyz. Este parámetro es opcional.

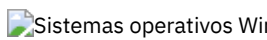
Al especificar un nombre o nombres de directorio, identifica las ubicaciones donde el servidor coloca los archivos que representan los volúmenes de almacenamiento para esta clase de dispositivo.

 Sistemas operativos AIX/Sistemas operativos Linux Al procesar el mandato, el servidor amplía el nombre o nombres de directorio especificados a forma completa, a partir del directorio raíz.

Importante: Si está utilizando agentes de almacenamiento para acceso compartido a volúmenes FILE, debe utilizar el mandato DEFINE PATH para definir una ruta para cada agente de almacenamiento. La definición de ruta incluye los nombres de directorio utilizados por el agente de almacenamiento para acceder a cada directorio.

Posteriormente, si el servidor necesita asignar un volumen reutilizable, crea un nuevo archivo en uno de estos directorios. (El servidor puede elegir cualquiera de los directorios para crear nuevos volúmenes reutilizables.) Para los volúmenes reutilizables que se utilizan para almacenar datos del cliente, el archivo que crea el servidor tiene la extensión de nombre de archivo .bfs. Para los volúmenes reutilizables que se utilizan para almacenar datos de exportación, se utiliza la extensión .exp.

 Sistemas operativos AIX/Sistemas operativos Linux Por ejemplo, si define una clase de dispositivo con un directorio de tsmstor y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine /tsmstor/00566497.exp.

 Sistemas operativos Windows Por ejemplo, si define una clase de dispositivo con un directorio de c:\server y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine c:\server\00566497.exp.

Consejo: Si especifica varios directorios para una clase de dispositivo, asegúrese de que los directorios están asociados con sistemas de archivos separados. Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio agregando valores que representan el espacio que queda en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar desactivado. Si un desencadenante se desactiva porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a activar el desencadenante con el siguiente mandato: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

Restricción: Para modificar una lista de directorios debe sustituir la lista completa.


SHAREd

Especifica si esta clase de dispositivo FILE se compartirá entre el servidor y uno o más agentes de almacenamiento. Para prepararse para el compartimiento, se definirá de manera automática una biblioteca junto con un número de unidades correspondiente al valor de MOUNTLIMIT asociado con la clase de dispositivo. Si la biblioteca y las unidades ya existen y el valor de MOUNTLIMIT se modifica, se pueden crear unidades para alcanzar un nuevo valor de MOUNTLIMIT más elevado o suprimir para obtener un nuevo valor más bajo.

Agentes de almacenamiento que utilizan volúmenes FILE

Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para acceder a los volúmenes FILE, los agentes de almacenamiento sustituyen los nombres de la lista de directorios en la definición de clase de dispositivo por los nombres de la lista de directorios de la definición de ruta asociada. A continuación, se muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:

 Sistemas operativos Windows

- c:\server
- d:\server
- e:\server

Sistemas operativos AIX

- /usr/tivoli1
- /usr/tivoli2
- /usr/tivoli3

Sistemas operativos Linux

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Utilice el siguiente mandato para configurar una biblioteca FILE denominada CLASSA con una unidad denominada CLASSA1 en SERVER1:

Sistemas operativos Windows

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

Sistemas operativos AIX

```
define devclass classa devtype=file
directory="/usr/tivoli1,/usr/tivoli2,/usr/tivoli3"
shared=yes mountlimit=1
```

Sistemas operativos Linux


```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```

2. Quiere que el agente de almacenamiento STA1 pueda utilizar la biblioteca FILE, para poder definir la siguiente ruta para el agente de almacenamiento STA1:

-  Sistemas operativos Windows


```
define path server1 stal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio c:\server por el nombre de directorio \\192.168.1.10\c\server para poder acceder a los volúmenes FILE que se encuentran en el directorio c:\server del servidor.

-  Sistemas operativos AIX

```
define path server1 stal srctype=server desttype=drive device=file
directory="/usr/ibm1,/usr/ibm2,/usr/ibm3" library=classa
```


En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio /usr/tivoli1 por el nombre de directorio /usr/ibm1 para poder acceder a los volúmenes FILE que se encuentran en el directorio /usr/tivoli1 del servidor.

-  Sistemas operativos Linux

```
define path server1 stal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```


En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio /opt/tivoli1 por el nombre de directorio /opt/ibm1/ para poder acceder a los volúmenes FILE que se encuentran en el directorio /opt/tivoli1 del servidor.

Se producen los resultados siguientes:

-  Sistemas operativos Windows SERVER1 crea el volumen de archivo c:\server\file1.dsm. Si cambia más adelante el primer directorio de la clase de dispositivo con el mandato siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```


SERVER1 todavía puede acceder al volumen de archivo c:\server\file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

-  Sistemas operativos AIX Si se crea el volumen de archivo /usr/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/usr/otherdir,/usr/tivoli2,  
/usr/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /usr/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

-  Sistemas operativos Linux Si se crea el volumen de archivo /opt/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,  
/opt/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /opt/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

Ejemplo: actualizar una clase de dispositivo FILE para su compartimiento


Preparar una clase de dispositivo FILE (denominada PLAINFILES) para compartirla con un agente de almacenamiento de IBM Spectrum Protect.

```
update devclass plainfiles shared=yes
```

Ejemplo: actualizar la capacidad de una clase de dispositivo FILE

Actualizar una clase de dispositivo FILE denominada STORFILES para establecer una capacidad máxima de 25 MB.

```
update devclass storfiles maxcap=25m
```

 Sistemas operativos AIX

Ejemplo: añadir un directorio a una clase de dispositivo FILE

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, /usr/otherdir, a la lista de directorios. Los directorios /opt/tivoli2 y /opt/tivoli3 se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa  
directory="/opt/tivoli2,/opt/tivoli3,/usr/otherdir"
```

 Sistemas operativos Linux

Ejemplo: añadir un directorio a una clase de dispositivo FILE

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, /usr/otherdir, a la lista de directorios. Los directorios /usr/tivoli2 y /usr/tivoli3 se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa  
directory="/usr/tivoli2,/usr/tivoli3,/usr/otherdir"
```

 Sistemas operativos Windows

Ejemplo: añadir un directorio a una clase de dispositivo FILE

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, c:\otherdir, a la lista de directorios. Los directorios d:\server y e:\server se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa
  directory="d:\server,e:\server,c:\otherdir"
```

 Sistemas operativos AIX  Sistemas operativos Windows

UPDATE DEVCLASS (Actualizar una clase de dispositivo GENERICTAPE)

Utilice la clase de dispositivo GENERICTAPE para las unidades de cinta admitidas por los controladores de dispositivo del sistema operativo.

Cuando se utiliza este tipo de dispositivo, el servidor no reconoce ningún tipo de dispositivo ni el formato de grabación de cartuchos. Dado que el servidor no reconoce el tipo de dispositivo, si se produce un error de E/S, la información de error será menos detallada en comparación con la información de error que se generaría para un tipo de dispositivo específico (por ejemplo, 8MM). Cuando defina dispositivos en el servidor, no combine varios tipos de dispositivos en el mismo tipo de dispositivo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+-----+----->
  '-ESTCAPacity----tamaño-'  '-MOUNTRetention----minutos-'
>--+-----+-----+----->
  '-MOUNTWait----minutos-'  '-MOUNTLimit----+DRIVES+-'
                               +-número+
                               '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Especifique una capacidad adecuada a la unidad de cintas determinada que esté utilizándose.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

UPDATE DEVCLASS (Actualizar una clase de dispositivo LTO)

Utilice la clase de dispositivo LTO cuando utilice dispositivos de cinta LTO.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+-----+----->
  '-LBProtect----+READWrite--+'
                    +-WRITEOnly-+
                    '-No-----'
>--+-----+-----+-----+----->
  '-FORMAT----+DRIVE----+'  '-ESTCAPacity---tamaño-'
                    +-ULTRIUM---+
                    +-ULTRIUMC--+
```

```

+-ULTRIUM2--+
+-ULTRIUM2C--+
+-ULTRIUM3--+
+-ULTRIUM3C--+
+-ULTRIUM4--+
+-ULTRIUM4C--+
+-ULTRIUM5--+
+-ULTRIUM5C--+
+-ULTRIUM6--+
'-ULTRIUM6C-'

>+-----+
'-PREFIX-----ADSM-----+'
    '-prefijo_volumen_cinta-'

>+-----+-----+-----+
'-MOUNTRetention-----minutos-' '-MOUNTWait-----minutos-'

>+-----+-----+
'-MOUNTLimit-----DRIVES--+
    +-número--+
    '-0-----'

>+-----+-----+-----+-----+
| (1) (2) |
'------DRIVEEncryption-----+ON-----+'
    +-ALLOW-----+
    +-EXTERNAL--+
    '-OFF-----'

```

Notas:

1. No puede especificar DRIVEENCRYPTION=ON si las unidades van a utilizar un medio WORM (una sola grabación, varias lecturas).
2. El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas LTO que utiliza esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de

calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: Se admite la protección de bloque lógico únicamente en IBM® LTO5 y unidades LTO6 soportadas.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. En su lugar, especifique el formato que utilizan las unidades.

Cuando migre todas las unidades de dispositivos Ultrium a dispositivos Ultrium 2:

- Suprima todas las definiciones de unidades Ultrium existentes y las rutas asociadas a ellas.
- Defina las nuevas unidades y rutas Ultrium 2.

Si piensa en mezclar distintas generaciones de unidades y medios LTO, tenga en cuenta las siguientes restricciones.

Tabla 1. Posibilidades de lectura/grabación para diferentes generaciones de unidades LTO

Unidades	Soporte de primera generación	Soporte de segunda generación	Soporte de tercera generación	Soporte de cuarta generación	Soporte de quinta generación	Soporte de sexta generación
Primera generación	Lectura y grabación	n/d	n/d	n/d	n/d	n/d
Segunda generación	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d	n/d
Tercera generación ¹	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d
Cuarta generación ²	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d
Quinta generación ³	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d
Sexta generación ⁴	n/d	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación

¹ En una biblioteca con una unidad de tercera generación, es necesario dar de baja todos los volúmenes reutilizables de primera generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de primera generación a sólo lectura.

² En una biblioteca con una unidad de cuarta generación, es necesario dar de baja todos los volúmenes reutilizables de segunda generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de segunda generación a sólo lectura.

³ En una biblioteca con una unidad de quinta generación, todos los volúmenes reutilizables de tercera generación se tienen que dar de baja y todos los volúmenes de agrupación de almacenamiento de tercera generación se tienen que actualizar a sólo lectura.

⁴ En una biblioteca con una unidad de sexta generación, es necesario dar de baja todos los volúmenes reutilizables de cuarta generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de cuarta generación a sólo lectura.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos LTO:

Tabla 2. Formato de grabación y capacidad estimada predeterminada para LTO

Formato	Capacidad estimada	Descripción
---------	--------------------	-------------

Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
ULTRIUM	100 GB	Formato sin comprimir, utilizando cartuchos Ultrium
ULTRIUMC	Consulte la nota 200 GB	Formato comprimido, utilizando cartuchos Ultrium
ULTRIUM2	200 GB	Formato sin comprimir (estándar) con cartuchos Ultrium 2
ULTRIUM2C	Consulte la nota 400 GB	Formato comprimido con cartuchos Ultrium 2
ULTRIUM3	400 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 3
ULTRIUM3C	Consulte la nota 800 GB	Formato comprimido, con cartuchos Ultrium 3
ULTRIUM4	800 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 4
ULTRIUM4C	Consulte la nota 1,6 TB	Formato comprimido con cartuchos Ultrium 4
ULTRIUM5	1,5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 5
ULTRIUM5C	Consulte la nota 3.0 TB	Formato comprimido con cartuchos Ultrium 5
ULTRIUM6	2.5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 6
ULTRIUM6C	Consulte la nota 6.25 TB	Formato comprimido con cartuchos Ultrium 6
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.		

ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información sobre capacidades estimadas, consulte Tabla 2.

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

Restricción: Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

Nota: No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (Si va a utilizar un soporte WORM, no puede especificar DRIVEENCRYPTION=ON).

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.



Ejemplo: actualizar el límite de montaje para una clase de dispositivo LTO

Actualizar una clase de dispositivo denominada LTOTAPE. Cambiar el límite de montaje a 2.

```
update devclass ltotape mountlimit=2
```

UPDATE DEVCLASS (Actualizar una clase de dispositivo NAS)

Utilice la clase de dispositivo NAS cuando realice operaciones con el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad de servidores de archivos de almacenamiento conectado a red (NAS). La clase de dispositivo es para las unidades a las que da soporte el servidor de archivos NAS para copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRary----nombre_biblioteca-'
>--+-----+----->
  '-MOUNTRetention---0-' '-MOUNTWait---minutos-'
>--+-----+----->
  '-MOUNTLimit---+DRIVES+' '-ESTCAPacity---tamaño-'
      +-numero+
      '-0-----'
>--+-----+-----<<
  '-PREFIX----prefijo_volumen_cinta-'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRary

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta SCSI utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

MOUNTRetention=0

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Cero (0) es el único valor admitido para clases de dispositivo con DEVType=NAS.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

Ejemplo: actualizar la capacidad estimada para una clase de dispositivo NAS.

Actualizar una clase de dispositivo denominada NASTAPE. Cambiar la capacidad estimada por 200 GB.

```
update devclass nastape library=naslib estcapacity=200G
```

UPDATE DEVCLASS (Actualizar una clase de dispositivo REMOVABLEFILE)

Utilice la clase de dispositivo REMOVABLEFILE para los dispositivos de medios extraíbles que están conectados como sistemas de archivos locales y extraíbles.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+-----+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+-----+-----+-----+-----+----->
  '-MAXCAPacity----tamaño-' '-MOUNTRetention----minutos-'
>--+-----+-----+-----+-----+-----+-----><
  '-MOUNTWait----minutos-' '-MOUNTLimit----+DRIVES++-'
                                     +-número+
                                     '-0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)



Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de medios extraíbles que puede utilizar esta clase de dispositivo. Este parámetro es opcional. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes definidos en una agrupación de almacenamiento clasificada por esta clase de dispositivo. Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Windows Dado que el servidor abre únicamente un archivo por medio físico extraíble, especifique una capacidad que permita que un archivo pueda utilizar totalmente la capacidad de su medio.

Debe especificar este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes).

Por ejemplo, MAXCAPACITY=5M especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 MB. El valor más pequeño permitido es 1 MB (es decir, MAXCAPACITY=1M).

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

UPDATE DEVCLASS Actualizar una clase de dispositivo SERVER)

Utilice la clase de dispositivo SERVER para utilizar los volúmenes de almacenamiento o los archivos archivados en otro servidor de IBM Spectrum Protect.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDdate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-SERVERName---nombre_servidor-'
>--+-----+----->
  '-MAXCAPacity---tamaño-'
>--+-----+----->
  '-PREFIX---+ADSM-----+-'
    '-prefijo_volumen_cinta-'
>--+-----+----->
  '-RETRYPeriod---minutos--'
>--+-----+----->
  '-RETRYInterval---seconds--'
>--+-----+----->
  '-MOUNTRetention---minutos-'
>--+-----+-----<<
  '-MOUNTLimit---+número+-'
    '-1-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

SERVERName

Especifica el nombre del servidor. El parámetro SERVERNAME debe coincidir con un servidor definido.

Nota: Si cambia SERVERNAME de un servidor existente a un nombre nuevo, los datos en el volumen bajo SERVERNAME antiguo ya no es accesible con esta clase de dispositivo.

MAXCAPacity

Especifica el tamaño máximo que los objetos pueden crear en el servidor destino. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor mínimo permitido es 1 MB (MAXCAPACITY=1M).

PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

RETRYPeriod

Especifica el período de reintento en minutos. El período de reintento es el intervalo de tiempo durante el cual el servidor debe intentar conectarse con un servidor destino, en caso de que se sospeche que existe un problema de comunicaciones. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

RETRYInterval

Especifica el intervalo de reintentos en segundos. El intervalo de reintentos es la frecuencia con la que se realizan los intentos dentro de un período de tiempo específico. Este parámetro es opcional. Puede especificar un número de 1 a 9999.

MOUNTRetention

Especifica el número de minutos que debe retenerse una conexión desocupada con el servidor de destino antes de que se cierre la conexión. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTLimit

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino. Los intentos de acceder a más sesiones de las que indica el límite de montaje harán que el emisor de la petición tenga que esperar. Este parámetro es opcional. Puede especificar un número de 1 a 4096.

Los siguientes son los valores posibles:

número

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino.

1

Especifica el número de sesiones simultáneas entre el servidor de origen y el servidor de destino.

UPDATE DEVCLASS (Actualizar una clase de dispositivo VOLSAFE)

Utilice el tipo de dispositivo VOLSAFE para trabajar con medios y unidades de la marca StorageTek VolSafe. Esta tecnología utiliza medios que no se pueden sobregabar. Por consiguiente, no emplee estos medios para copias de seguridad a corto plazo de archivos de cliente, la base de datos de servidor o cintas de exportación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY-----nombre_biblioteca-'
>--+-----+-----+----->
  '-FORMAT-----+--DRIVE-----+'  '-ESTCAPacity-----tamaño-'
      +-9840-----+
      +-9840-C-----+
      +-T9840C-----+
      +-T9840C-C---+
      +-T9840D-----+
      +-T9840D-C---+
      +-T10000A-----+
      +-T10000A-C-+
      +-T10000B-----+
      +-T10000B-C-+
      +-T10000C-----+
      +-T10000C-C-+
      +-T10000D-----+
      +-T10000D-C-'
>--+-----+----->
  '-PREFIX-----+--ADSM-----+'
      '-prefijo_volumen_cinta-'
>--+-----+-----+----->
  '-MOUNTRetention-----minutos-'  '-MOUNTWait-----minutos-'
>--+-----+-----+-----<
  '-MOUNTLimit-----+--DRIVES--+-'
      +-número-+
      '+_0-----'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas VolSafe que puede utilizar esta clase de dispositivo. Si alguna unidad de una biblioteca está activada para VOLSafe, todas las unidades de la biblioteca deben activarse para VOLSafe. Para obtener más información acerca del tipo de dispositivo VolSafe, consulte DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE).

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Atención: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos VolSafe:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para cintas volsafe

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
9840	20 GB	Formato sin comprimir (estándar), cuando se utiliza un cartucho de 20 GB de 270 metros (885 pies) de cinta

Formato	Capacidad estimada	Descripción
9840-C	80 GB	Formato comprimido ampliado LZ-1 (4:1), cuando se utiliza un cartucho de 80 GB con 270 metros (885 pies) de cinta
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS)

Utilice este mandato para actualizar una clase de dispositivo. Hay disponible un conjunto limitado de tipos de clase de dispositivo para los dispositivos a los que se accede mediante un servidor de medios de z/OS.

- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS)

Tabla 1. Mandatos relacionados con UPDATE DEVCLASS

Mandato	Descripción
---------	-------------

Mandato	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE DEVCLASS (servidor de medios de z/OS)	Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS)

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a dispositivos 3590. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```

(1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
' -LIBRARY----nombre_biblioteca-'
>--+-----+----->
' -FORMAT-----DRIVE----' ' -ESTCAPacity----tamaño-'
      +-3590B---+
      +-3590C---+
      +-3590E-B--+
      +-3590E-C--+
      +-3590H-B--+
      '-3590H-C-'
>--+-----+----->
' -COMpression-----+Yes-+-'
      '-No--'
>--+-----+----->
' -MOUNTRetention----minutos-' ' -MOUNTWait----minutos-'
>--+-----+----->
' -MOUNTLimit-----+DRIVES-+-' ' -EXPIration----yyyyddd-'
      +-número-+
      '-0-----'
>--+-----+----->
' -RETention----días-' ' -PROtection-----+No-----+-'
      +-Yes-----+
      '-Automatic-'
>--+-----+-----<<
' -UNIT----nombre_unidad-'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.

2. No puede actualizar el parámetro PREFIX con este mandato. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

En la tabla siguiente se muestra una lista de las opciones de formato de grabación de los dispositivos 3590:

Tabla 1. Formatos de grabación para 3590

Formato	Descripción
3590B	Formato sin comprimir (básico)
3590C	Formato comprimido
3590E-B	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Formato comprimido, similar al formato 3590C
3590H-B	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Formato comprimido, similar al formato 3590C
Nota: Si el formato utiliza la función de compresión por hardware de la unidad de cintas, la capacidad real puede disminuir, dependiendo de la eficacia de la compresión.	

ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la

petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como *2014007* (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto de cero para el parámetro RETENTION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que dé soporte a la cinta 3590. Este parámetro es opcional. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS)

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a dispositivos 3592. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
(1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+-----+-----+-----+----->
  '-LIBRARY----biblioteca_medio_zos-'
>--+-----+-----+-----+-----+-----+----->
  '-FORMAT-----DRIVE----+' '-ESTCAPacity----tamaño-'
      +-3592----+
      +-3592C---+
      +-3592-2---+
      +-3592-2C--+
      +-3592-3---+
      +-3592-3C--+
      +-3592-4---+
      '-3592-4C-'
>--+-----+-----+-----+-----+-----+----->
  '-COMPression-----+Yes-+-'
```

```

'-No--'
>----->
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
>----->
'-MOUNTLimit---+DRIVES+-' '-EXPIration---yyyyddd-'
      +-número+
      '-0-----'
>----->
'-RETention---días-' '-PROtection---+No-----+-'
                        +-Yes-----+
                        '-Automatic-'
>-----<
'-UNIT---nombre_unidad-'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.
2. No puede actualizar el parámetro PREFIX con este mandato. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3592

Formato	Descripción
3592	Formato sin comprimir (básico)
3592C	Formato comprimido
3592-2	Formato sin comprimir (básico), similar al formato 3592
3592-C	Formato comprimido, similar al formato 3592C
3592-3	Formato sin comprimir (básico), similar al formato 3592
3592-3C	Formato comprimido, similar al formato 3592C
3592-4	Formato sin comprimir (básico), similar al formato 3592
3592-4C	Formato comprimido, similar al formato 3592C
DRIVE	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser distinta del valor que aparece en la lista.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades. Para un resultado óptimo, no mezcle las generaciones de unidades en la misma

biblioteca. Si una biblioteca contiene una mezcla de generaciones, pueden darse problemas en los medios. Por ejemplo, las unidades de primera generación y segunda generación no pueden leer medios de tercera generación. Si es posible, actualice todas las unidades a 3592 de tercera generación. Si no puede actualizar todas las unidades a 3592 de tercera generación, debe utilizar una configuración especial.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: **K** (KB), **M** (MB), **G** (GB) o **T** (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como *2014007* (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto de cero para el parámetro RETENTION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cintas que dé soporte a la cinta 3592. Este parámetro es opcional. Este nombre puede tener un máximo de 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a unidades StorageTek como, por ejemplo, StorageTek T9840 o T10000. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
(1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>+-----+----->
  '-LIBRARY----biblioteca_medio_zos-'
>+-----+-----+-----+----->
  '-FORMAT----+--DRIVE----+'  '-ESTCAPacity----tamaño-'
      +-T9840C----+
      +-T9840C-C--+
      +-T9840D----+
      +-T9840D-C--+
      +-T10000A----+
      +-T10000A-C--+
      +-T10000B----+
      +-T10000B-C--+
      +-T10000C----+
      +-T10000C-C--+
      +-T10000D----+
      '-T10000D-C-'
>+-----+-----+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>+-----+-----+-----+----->
  '-MOUNTLimit----+--DRIVES--+-'  '-COMPRESSION----+--Yes--+-'
      +-número--+
      '-0-----'
      '-No--'
>+-----+-----+-----+----->
  '-EXPIRATION---yyyyddd-'  '-RETENTION---días-'
>+-----+-----+-----+----->
  '-PROTECTION----+--No-----+-'
      +-Yes-----+
      '-Automatic-'
>+-----+-----+-----+-----><
  '-UNIT----nombre_unidad-'
```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.
2. No puede actualizar el parámetro PREFIX con este mandato. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. DRIVE es el valor predeterminado. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
Nota:		
<ul style="list-style-type: none">Algunos formatos utilizan una función de compresión del hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C.		

ESTCAPacity

Especifica la capacidad estimada para los volúmenes de acceso secuencial que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es

100 KB (ESTCAPACITY=100K).

MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como *2014007* (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto de cero para el parámetro RETENTION.

PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite mandatos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los mandatos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que den soporte a las cintas ECARTRIDGE. Utilice el nombre de la unidad que representa el subconjunto de unidades de la biblioteca que están conectadas al sistema z/OS. Este parámetro es opcional. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS)

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a archivos en el almacenamiento de disco magnético como volúmenes de acceso secuencial (como en una cinta). La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

Un volumen en esta clase de dispositivo es un conjunto de datos lineal VSAM (Virtual Storage Access Method) al que accede el servidor de medios de z/OS. Se pueden utilizar los volúmenes reutilizables con una clase de dispositivo y el servidor de medios de z/OS asignará

dinámicamente el conjunto de datos lineal VSAM. No es necesario definir volúmenes para que el servidor utilice la clase de dispositivo. Si define volúmenes, establezca el calificador de alto nivel (HLQ) para que SMS reconozca la solicitud de asignación del servidor de medios de z/OS. Si utiliza volúmenes definidos, la función formatear volúmenes no se admite para el servidor al utilizar esta clase de dispositivo. El servidor de medios de servidor de medios de z/OS z/OS utiliza una característica FormatWrite del gestor de medios DFSMS al llenar los volúmenes FILE.

Puede definir los volúmenes para la clase de dispositivo FILE utilizando el mandato DEFINE VOLUME. No obstante, el servidor de medios de z/OS no asigna espacio para un volumen definido hasta que se abra el volumen para su primer uso.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->>
>--+-----+-----+-----+-----+----->
  '-MAXCAPacity----tamaño-' '-PRIMARYalloc----tamaño-'
>--+-----+-----+-----+-----+----->
  '-SECONDARYalloc----tamaño-'
>--+-----+-----+-----+-----+----->
  '-PREFIX----prefijo_volumen_archivo-'
>--+-----+-----+-----+-----+-----<<
  '-MOUNTLimit----numero-'
```

Parámetros

nombre_clase_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes de archivos definidos en una agrupación de almacenamiento de esta clase de dispositivo. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc

Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen. Debe haber disponible suficiente espacio para satisfacer la cantidad de asignación primaria. La política SMS (Storage Management Subsystem) determina si se pueden utilizar varios volúmenes físicos para satisfacer la petición de asignación primaria.

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 100 KB (PRIMARYALLOC=100K). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G). Todos los valores se redondean al siguiente múltiple superior de 256 K.

Para evitar espacio desaprovechado, la operación de asignación dinámica utiliza el menor de los valores especificados en los dos parámetros PRIMARYALLOC y MAXCAPACITY.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

SECONDARYalloc

Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado. El conjunto de datos de un volumen de archivos se amplía al tamaño establecido por el parámetro MAXCAPACITY y, a continuación, el volumen se marca como lleno.

Como la asignación secundaria de un conjunto de datos lineal no puede ocupar un volumen físico, tenga en cuenta el tamaño del volumen físico al seleccionar un tamaño de asignación secundaria. Por ejemplo, los volúmenes físicos de un modelo 3 de 3390 tienen aproximadamente 2,8 GB. Para garantizar que cada petición ocupe prácticamente un volumen físico completo, pero no más, utilice un tamaño de asignación secundario que sea un poco menor de 2,8 GB. Una cantidad de asignación secundaria de

2600 MB permite suficiente espacio para el conjunto de datos de volumen VSAM (VVDS), la etiqueta de volumen y la tabla de índice de volumen (VTOC).

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El valor mínimo es 0 KB (SECONDARYALLOC=0K). El valor máximo es 16384 GB. Excepto 0, todos los valores se redondean al siguiente múltiple superior de 256 K.

Si se especifica 0 (SECONDARYALLOC=0), el volumen de archivo no se puede ampliar más allá de la cantidad de asignación primaria.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

Si especifica un valor para el parámetro SECONDARYALLOCATION que no es 0, o si permite que el valor tome como valor predeterminado 2600M, la DATACLAS SMS asociada al identificador PREFIX (por ejemplo, calificador de alto nivel) debe tener especificado el atributo Extended Addressability (EA). Sin el atributo EA, la DATACLAS SMS limita la asignación del volumen FILE del conjunto de datos lineal VSAM a la ampliación primaria. (Consulte la descripción del parámetro PRIMARYALLOCATION). Con el conjunto de datos limitado al tamaño de asignación primario, el servidor de medios de z/OS no puede ampliar el conjunto de datos y el volumen se marca como FULL antes de que se alcance la capacidad máxima.

Restricción: Asegúrese de que los valores especificados para los parámetros PRIMARYALLOC y SECONDARYALLOC entren en los límites prácticos del dispositivo de almacenamiento. El servidor no puede comprobar si los valores exceden los límites prácticos del dispositivo y tampoco comprueba si los dos valores exceden conjuntamente el valor de MAXCAPACITY actual. Consejo: Para rellenar los volúmenes cuando especifica un valor elevado para el parámetro MAXCAPACITY, especifique valores elevados para los parámetros PRIMARYALLOC y SECONDARYALLOC. Utilice tamaños de volumen de MVS mayores para reducir la posibilidad de anomalías de ampliación.

PREFIX

Especifica el calificador de nivel superior del nombre del conjunto de datos que se utiliza para asignar conjuntos de datos de volúmenes reutilizables. Para todos los volúmenes de archivos reutilizables creados en esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima del prefijo, incluidos los puntos, es de 32 caracteres.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de conjunto de datos de volumen de archivo que utilice el prefijo predeterminado es

```
ADSM.B0000021.BFS.
```

Si tiene un convenio de denominación de conjunto de datos, utilice un prefijo que se ajuste a sus convenios de denominación. Por ejemplo, el siguiente valor es aceptable: TSM.SERVER2.VSAMFILE.

Si ejecuta varias instancias de servidor para IBM Spectrum Protect o Tivoli Storage Manager for z/OS Media, debe utilizar un valor exclusivo para el parámetro PREFIX para cada clase de dispositivo que actualice.

MOUNTLimit

Especifica el número máximo de volúmenes FILE que se pueden abrir simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Para los dispositivos 3995 que emulan dispositivos 3390, el valor no debe establecerse en un número mayor que el número de corrientes de entrada y salida concurrentes que pueden existir en el medio que almacena los volúmenes.

El valor que especifique en este parámetro es importante si existe una importante penalización al conmutar de un volumen a otro. Por ejemplo, la conmutación puede llevarse a cabo cuando se utilizan dispositivos IBM® 3995 que emulan dispositivos 3390. El valor que especifique no puede ser mayor que el número de unidades físicas disponibles en el dispositivo.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

UPDATE DOMAIN (Actualizar un dominio de políticas)

Utilice este mandato para cambiar un dominio de políticas.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas especificado.

Sintaxis

```
>>-UPDate Domain--nombre_dominio----->
>-----+-----+----->
'-DESCRiption----descripción-'
>-----+-----+-----+----->
'-BACKRETention----días-' '-ARCHRETention----días-'
>-----+-----+-----+----->
|                                     |
|                                     |
|                                     |
'-ACTIVEDESTination-----nombre_agrupación_datos_activos-----+'
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas.

DESCRiption

Describe el dominio de políticas utilizando una serie de texto. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("").

BACKRETention

Especifica el número de días (a partir de la fecha en que quedaron inactivas las versiones de copia de seguridad) que deben retenerse las versiones de copia de seguridad que ya no están en el sistema de archivos del cliente. Este parámetro es opcional. Puede especificar un entero en el rango 0 – 9999. El servidor utiliza el valor de retención de copia de seguridad para gestionar las versiones inactivas de archivos cuando se producen cualquiera de las condiciones siguientes:

- Un archivo se vuelve a vincular a una nueva clase de gestión, pero ni la nueva clase de gestión ni la clase de gestión predeterminada contienen un grupo de copia de seguridad.
- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.

ARCHRETention

Especifica el número de días (desde la fecha de archivado) que se han de retener las copias archivadas. Este parámetro es opcional. Puede especificar un entero entre 0 y 30.000. El servidor utiliza el valor de retención de copias archivadas para gestionar las copias archivadas cuando se produce una de las condiciones siguientes:

- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia archivada.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia archivada.

ACTIVEDESTination

Especifica los nombres de las agrupaciones de datos activos que almacenan versiones activas de datos de copias de seguridad para nodos asignados al dominio. Este parámetro es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos. Como máximo, puede especificar diez agrupaciones de datos activos para un dominio.

Antes de que el servidor de IBM Spectrum Protect grabe datos en una agrupación de datos activos, verifica si el nodo que posee los datos se ha asignado a un dominio que tiene la agrupación de datos activos que se indica en la lista ACTIVEDESTINATION. Si el servidor comprueba que el nodo cumple estos criterios, los datos se almacenarán en la agrupación de datos activos. Si el nodo no cumple los requisitos, los datos no se almacenarán en la agrupación de datos activos. Si la función de grabación simultánea se utiliza para grabar datos en una agrupación de almacenamiento de datos activos, el servidor realiza la verificación durante operaciones de copia de seguridad de clientes de archivado y copia de seguridad de IBM Spectrum Protect o de clientes

de aplicación mediante la API de IBM Spectrum Protect. La verificación también se realiza cuando se copian datos activos con el mandato COPY ACTIVATEDATA.

Ejemplo: actualizar el período de retención de copia de seguridad de un dominio de políticas

Actualice el dominio de políticas ENGPOLDOM de manera que el período de gracia de retención de copia de seguridad se amplíe a 90 días y el de archivado a dos años. Especifique una agrupación de datos activos como destino para versiones activas de datos de copia de seguridad que pertenecen a los nodos que están asignados al dominio. Utilice *engactivedata* como nombre de la agrupación de datos activos. Emita el mandato siguiente:

```
update domain engpoldom description='Dominio de políticas de Ingeniería'  
backretention=90 archretention=730 activedestination=engactivedata
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE DOMAIN




Mandato	Descripción
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.

UPDATE DRIVE (Actualizar una unidad)

Utilice este mandato para actualizar una unidad.

Clase de privilegio

Si quiere obtener información detallada y actual sobre el soporte de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate DRive--nombre_biblioteca--nombre_unidad----->  
>--+-----+-----+-----+----->  
  '-SERial---+--número_serie--+'  '-ONLine---+--Yes--+'  
          '-AUTODetect---'          '-No--'  
>--+-----+-----+-----+----->  
  '-ELEMeNt---+--dirección--+'  
          '-AUTODetect-'  
>--+-----+-----+-----+----->  
  |                               (1) |  
  '-ACSDRVID---+--id_unidad-----'  
>--+-----+-----+-----+-----><  
  |                               (2) |  
  '-CLEANFREQuency---+--NONE-----+ |  
                    |               (3) |  
                    +-ASNEEDED-----+  
                    '-gigabytes----'
```

Notas:

1. El parámetro ACSDRVID sólo es válido para unidades de las bibliotecas ACSLS.
2. El parámetro CLEANFREQUENCY sólo es válido para unidades de las bibliotecas SCSI.
3. El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona para todas las unidades de cintas. Si desea obtener más información, consulte la descripción del parámetro.

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca a la que se asigna la unidad.

nombre_unidad (Obligatorio)

Especifica el nombre asignado a la unidad.

SERial

Especifica el número de serie de las unidades que están actualizándose. Este parámetro sólo es válido para las unidades en una biblioteca de cintas virtual (VTL) o SCSI. Este parámetro es opcional. Los valores posibles son:

número_serie

Especifica el número de serie de la unidad que está actualizándose.

Nota: Si ya se ha definido una ruta para esta unidad, el número que entra aquí se compara con el número detectado por IBM Spectrum Protect. Si los números no coinciden, el mandato no se ejecuta correctamente.

AUTODETECT

Especifica que IBM Spectrum Protect detecta y utiliza automáticamente el número de serie si ya se ha definido una ruta a esta unidad.

Si no se ha definido una ruta a esta unidad, no se detecta el número de serie.

ONLine

Especifica si la unidad está disponible para utilizarla. Este parámetro especifica si las unidades se pueden poner fuera de línea y utilizarse para otra actividad, por ejemplo mantenimiento. Este parámetro es opcional.

Puede emitir este mandato cuando la unidad esté relacionada en un proceso activo o sesión, pero no se recomienda. Si emite un mandato para que la unidad pase a un estado desactivado mientras está en uso, se emitirá un mensaje de error. El volumen montado completa su proceso actual. Si este volumen formaba parte de una serie de volúmenes para una transacción específica, la unidad no está disponible para finalizar el montaje de la serie. Si no hay ninguna otra unidad disponible, el proceso fallará.

Atención: Cuando se utilice una unidad, no especifique el parámetro ELEMENT con el parámetro ONLINE. La unidad no se actualiza y el mandato falla.

El estado de la unidad no cambiará aunque detenga y reinicie el servidor. Si una unidad está desactivada cuando se reinicia el servidor, se emite un mensaje de aviso que indica que la unidad debe activarse manualmente. Si todas las unidades de una biblioteca se actualizan para estar desactivadas, los procesos que necesitan un punto de montaje de biblioteca fallan, en lugar de hacer cola para obtener un punto de montaje.

YES

Especifica que la unidad está disponible para utilizarla (activada).

No

Especifica que la unidad no está disponible para utilizarla (desactivada).

ELEMent

Especifica la dirección del elemento de la unidad dentro de una biblioteca SCSI o VTL. El servidor utiliza la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Este parámetro solo es válido para una unidad de una biblioteca SCSI o VTL cuando se emite el mandato desde un servidor de gestor de bibliotecas de IBM Spectrum Protect. Los valores posibles son:

dirección

Especifica la dirección de elemento de la unidad que está actualizándose.

Para localizar la dirección del elemento para la configuración de la biblioteca, consulte la información del fabricante.

Recuerde: Si ya se ha definido una ruta a esta unidad, el número que entre aquí se comparará con el número detectado anteriormente por IBM Spectrum Protect. Si los números no coinciden, este mandato no se ejecuta correctamente.

AUTODETECT

Especifica que IBM Spectrum Protect detecta y utiliza automáticamente el número de elemento si ya se ha definido una ruta a esta unidad.

Si no se ha definido una ruta a esta unidad, no se detecta el número de elemento.

Restricción: Si la biblioteca en la que se encuentra la unidad no admite el mandato SCSI Read Element Status, y ELEMENT=AUTODETECT, el mandato no se ejecuta correctamente y genera un mensaje de error de IBM Spectrum Protect.

ACSDRVID

Especifica el ID de la unidad a la que se accede en una biblioteca SCSI. El identificador de unidad es un conjunto de números que indica la ubicación física de una unidad dentro de una biblioteca ACSLS. Este identificador de unidad debe especificarse como *a,l,p,d*, siendo *a* el ACSID, *l* el LSM (módulo de almacenamiento de biblioteca, *p* el número de panel y *d* el ID de unidad. El servidor necesita el identificador de unidad para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Consulte la documentación de StorageTek para obtener más detalles.

CLEANFREQUENCY

Especifica la frecuencia con que el servidor activa la limpieza de la unidad. Este parámetro es opcional. Para conseguir el grado de automatización de limpieza más completo para una biblioteca automatizada, deberá tener un cartucho limpiador dado de alta en el inventario de volúmenes de la biblioteca. Si va a utilizar una limpieza en función de la biblioteca, se recomienda NONE cuando el tipo de biblioteca es compatible con esta función. Este parámetro sólo es válido para unidades en bibliotecas SCSI y no es válido para bibliotecas gestionadas externamente, por ejemplo bibliotecas 3494 o bibliotecas StorageTek que se gestionan bajo ACSLS.

Importante: Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades activada por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

NONE

Especifica que el servidor no hace el seguimiento de la limpieza de esta unidad. Utilice este parámetro para las bibliotecas que tengan su propia limpieza automática.

ASNEEDED

Especifica que el servidor sólo carga la unidad con un cartucho limpiador dado de alta cuando una unidad notifica al controlador de dispositivo que es necesaria la limpieza.

El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Visite el sitio web Dispositivos soportados correspondiente a su sistema operativo. Si ASNEEDED no está soportado, puede utilizar el valor gigabytes para la limpieza automática.

Con los controladores IBM 3592 e LTO, se recomienda la limpieza en función de la biblioteca. Si no es compatible la limpieza en función de la biblioteca, debe utilizarse ASNEEDED. Gigabytes no es recomendable.

Restricción: IBM Spectrum Protect no controla las unidades conectadas al servidor de archivos NAS. Si hay una unidad conectada sólo a un servidor de archivos NAS (no a un servidor o agente de almacenamiento), no especifique ASNEEDED como frecuencia de limpieza.

gigabytes

Especifica, en gigabytes, la cantidad de datos procesada en la unidad antes de que el servidor cargue la unidad con un cartucho limpiador. El servidor restablece el contador de gigabytes procesados cada vez que carga un cartucho limpiador en la unidad.

Importante: Cuando CLEANFREQUENCY=gigabyte, se puede producir la limpieza de unidad antes de que se alcance el valor de gigabytes, si la unidad notifica al controlador de dispositivo que es necesaria una limpieza.

Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si la información ofrece las recomendaciones para la frecuencia de limpieza en términos de horas de uso, convierta el valor en gigabytes realizando lo siguiente:

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor en gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.

Consejo: En el caso de IBM 3590, especifique un valor para la frecuencia de limpieza con el fin de garantizar que las unidades reciben la limpieza adecuada. Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si utiliza la frecuencia de limpieza que recomienda IBM, las unidades no se limpian más de lo necesario.

Ejemplo: actualizar la dirección de elemento de una unidad

Actualizar DRIVE3, en la biblioteca denominada AUTO, cambiando la dirección de elemento a 119.

```
update drive auto drive3 element=119
```

Ejemplo: desactivar una unidad

Actualizar DRIVE3, en la biblioteca denominada MANLIB, para dejarla fuera de línea.

update drive manlib drive3 online=no

Mandos relacionados

Tabla 1. Mandatos relacionados con UPDATE DRIVE

Mandato	Descripción
CLEAN DRIVE	Marca una unidad para limpiarla.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE PATH	Cambia los atributos asociados con una ruta.

UPDATE FILESPACE (Actualizar reglas de réplica de nodos de espacio de archivos)

Utilice este mandato para actualizar las reglas de réplica de espacio de archivos. También puede activar o desactivar la réplica de datos a la que se aplica una regla de espacio de archivos.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el nodo cliente con el espacio de archivos que se va a actualizar.

Sintaxis

```
>>-UPDate Filespace--nombre_nodo--nombre_espacio_archivos----->
.-NAMEType-----SERVER-----
>+-----+-----+-----+-----+----->
'-NAMEType-----+SERVER-----+'
      +UNICODE--+
      | (1) |
      '-FSID-----'

.-CODEType-----BOTH-----
>+-----+-----+-----+-----+----->
'-CODEType-----+UNICODE-----+'
      +NONUNICODE--+
      '-BOTH-----'

.-,-----,
v               (2) |
>>-DATAType-----+BACKup-----+----->
      +ARCHive-----+
      '-SPACEManaged-'

>+-----+-----+-----+-----+----->
|               (3) |
'-REPLRule-----+ALL_DATA-----+'
      |               (4) |
      +-ACTIVE_DATA-----+
      +-ALL_DATA_HIGH_PRIORITY-----+
      |               (4) |
      +-ACTIVE_DATA_HIGH_PRIORITY-----+
      +-DEFAULT-----+
      '-NONE-----'

>+-----+-----+-----+-----+----->
|               (3) |
```

```
'-REPLState--=-----+Enabled---+-----'  
      +-DISabled--+  
'-PURGEdata-'
```

Notas:

1. No puede especificar un identificador de espacio de archivos (FSID) si utiliza caracteres comodín para el nombre del nodo de cliente.
2. Sólo puede especificar cada regla una vez.
3. Debe especificar el parámetro REPLRULE o el parámetro REPLSTATE en este mandato.
4. Las reglas ACTIVE_DATA y ACTIVE_DATA_HIGH_PRIORITY son válidas solo si especifica DATATYPE=BACKUP.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nodo cliente al que pertenece el espacio de archivos. Puede utilizar caracteres comodín para especificar este nombre. No obstante, los identificadores de espacios de archivos pueden ser distintos entre los nodos de cliente del mismo espacio de archivos. Por lo tanto, no puede especificar caracteres comodín para el nombre del nodo de cliente y el FSID como el valor del parámetro NAMETYPE.

nombre_espacio_archivos (Necesario)

Especifica el nombre del espacio de archivos que se va a actualizar. Puede utilizar caracteres comodín o una lista delimitada por comas para especificar nombres.

Para un servidor que tenga clientes con espacios de archivos activados para Unicode, puede que deba hacer que el servidor convierta el nombre del espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta un nombre de la página de códigos del servidor a Unicode. Para obtener información adicional, consulte el parámetro NAMETYPE. Si sólo especifica un solo carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a espacios de archivos no Unicode.

Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos que se va a actualizar, utilice el mandato QUERY FILESPACE.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y tienen sistemas operativos de Windows, Macintosh OS X o NetWare.

Utilice este parámetro sólo si especifica un nombre de espacio de archivos parcial o totalmente calificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende del sistema operativo, los caracteres que contiene el nombre y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión falla, el nombre puede contener signos de interrogación, espacios en blanco o puntos suspensivos (...).

FSID

El servidor interpreta los nombres de los espacios de archivos como identificadores de espacios de archivos.

CODETYPE

Especifica el tipo de espacios de archivos que se van a incluir en el proceso de réplica de nodos. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

UNICODE

Especifica sólo los espacios de archivos que están en Unicode.

NONUNICODE

Especifica sólo los espacios de archivos que no están en Unicode.

BOTH

Especifica todos los espacios de archivos independientemente del tipo de página de códigos.

DATATYPE (obligatorio)

Especifica el tipo de datos al que se aplica una regla de réplica. Para especificar varios tipos de datos, separe los nombres con comas y sin espacios intercalados. Puede especificar los siguientes valores:

BACKup

Especifica el tipo de datos de copia de seguridad.

ARCHive

Especifica el tipo de datos de archivado.

SPACEManaged

Especifica el tipo de datos gestionados por espacio.

REPLRule

Especifica la regla de réplica que se aplica a un tipo de datos. No puede utilizar comodines. Si especifica varios tipos de datos, la regla de réplica se aplica a cada tipo de datos. Por ejemplo, si especifica `DATATYPE=BACKUP, ARCHIVE`, la regla de réplica se aplica a los datos de copia de seguridad y a los datos de archivado.

Restricción: El parámetro `REPLRULE` es opcional. No obstante, si no lo especifica, debe especificar el parámetro `REPLSTATE`.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que un espacio de archivos contiene datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a los datos de copia de seguridad activos, especifique `DATATYPE=BACKUP REPLRULE=ACTIVE_DATA_HIGH_PRIORITY`. Para asignar una prioridad normal a los datos de archivado, vuelva a emitir el mandato `UPDATE FILESPACE` y especifique `DATATYPE=ARCHIVE REPLRULE=ALL_DATA`.

Puede especificar las reglas siguientes:

ALL_DATA

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Sólo replica datos de copia de seguridad activos en un espacio de archivos. Los datos se replican con una prioridad normal.

Atención: Si especifica `ACTIVE_DATA` y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato `REPLICATE NODE` con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL_DATA_HIGH_PRIORITY

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica `ACTIVE_DATA` excepto que los datos se replican con una prioridad alta.

DEFAULT

Los datos se replican de acuerdo con la regla de nodo de cliente para el tipo de datos.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es especificar `DATATYPE=ARCHIVE REPLRULE=DEFAULT` para cada espacio de archivos. Asegúrese de que la regla de réplica del cliente de los datos de archivado esté establecida en `ALL_DATA_HIGH_PRIORITY` o en `DEFAULT`. Si la regla de réplica del cliente es `DEFAULT`, la regla de réplica del servidor para los datos de archivado debe establecerse en `ALL_DATA_HIGH_PRIORITY`.

NONE

No se replican datos. Por ejemplo, si no desea replicar los datos gestionados por espacio en un espacio de archivos, especifique `DATATYPE=SPACEMANAGED REPLRULE=NONE`.

REPLState

Especifica el estado de réplica de un tipo de datos. Si ha especificado varios tipos de datos, el estado se aplica a todos los tipos de datos. Por ejemplo, si ha especificado `DATATYPE=BACKUP, ARCHIVE`, el estado se aplica a los datos de copia de seguridad y a los datos de archivado.

El parámetro `REPLSTATE` es opcional. No obstante, si no lo especifica, debe especificar el parámetro `REPLRULE`. Puede especificar uno de los siguientes valores para el parámetro `REPLSTATE`:

ENabled

Especifica que el tipo de datos está preparado para la réplica.

DISabled

Especifica que la réplica no se realiza hasta que la activa.

PURGEdata

Especifica que los datos se suprime del servidor de réplica de destino. El tipo de datos suprimido es el tipo de datos especificado por el parámetro `DATATYPE`. Por ejemplo, si especifica `DATATYPE=BACKUP, ARCHIVE` y `REPLSTATE=PURGEDATA`, los datos de copia de seguridad y los datos de archivado se suprimen del espacio de archivos en el servidor de réplica de destino.

Una vez suprimidos los datos, el parámetro `REPLSTATE` se establece en `DISABLED`, lo que impide la réplica en el futuro del tipo o los tipos de datos. La regla de réplica del tipo de datos se establece en `DEFAULT`.

Recuerde: El proceso de `PURGEDATA` no suprime los espacios de archivos. Sólo se suprimen los datos. El espacio de archivos aparece como vacío en la salida del mandato `QUERY OCCUPANCY`.

Ejemplo: actualizar las reglas de réplica de dos tipos de datos

`NODE1` tiene tres espacios de archivos: `/a`, `/b` y `/c`. Las reglas de réplica de todos los espacios de archivos se establecen en `ALL_DATA`. No obstante, desea replicar los datos de copia de seguridad y archivado en el espacio de archivos `/a` antes de replicar los datos en los otros espacios de archivos.

```
update filespace node1 /a datatype=backup,archive replrule=
all_data_high_priority
```

Ejemplo: actualizar las reglas de réplica de dos tipos de datos

`NODE2` tiene dos espacios de archivos: `/a` y `/b`. Desea suspender temporalmente la réplica de todos los datos en el espacio de archivos `/b`.

```
update filespace node2 /b datatype=backup,archive,spacemanaged
replstate=disabled
```



Mandatos relacionados


Tabla 1. Mandatos relacionados con `UPDATE FILESPACE`

Mandato	Descripción
<code>QUERY FILESPACE</code>	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
<code>QUERY NODE</code>	Visualiza información parcial o completa sobre uno o más clientes.
<code>QUERY REPLICATION</code>	Muestra información sobre los procesos de réplica de nodos.
<code>QUERY STATUS</code>	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos <code>SET</code> .
<code>REPLICATE NODE</code>	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
<code>SET REPLRETENTION</code>	Especifica el periodo de retención de los registros de historial de réplicas.
<code>UPDATE NODE</code>	Cambia los atributos que están asociados con un nodo de cliente.
<code>UPDATE REPLRULE</code>	Activa o desactiva las reglas de réplica.
<code>VALIDATE REPLICATION</code>	Verifica la réplica para los espacios de archivos y los tipos de datos.

UPDATE LIBRARY (Actualizar una biblioteca)

Utilice este mandato para actualizar una definición de biblioteca.




 Sistemas operativos AIX  Sistemas operativos Windows Para actualizar el nombre de dispositivo, el número ACS o el nombre de ruta del gestor externo de una biblioteca, debe emplear el mandato UPDATE PATH.

 Sistemas operativos Linux Para actualizar el nombre de dispositivo o el nombre de ruta del gestor externo de una biblioteca, debe emplear el mandato UPDATE PATH.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de biblioteca.

- UPDATE LIBRARY (Actualizar una biblioteca 349X)
- UPDATE LIBRARY (Actualizar una biblioteca ACSLS)
- UPDATE LIBRARY (Actualizar una biblioteca EXTERNAL)
- UPDATE LIBRARY (Actualizar una biblioteca FILE)
- UPDATE LIBRARY (Actualizar una biblioteca manual)
- UPDATE LIBRARY (Actualizar una biblioteca SCSI)
- UPDATE LIBRARY (Actualizar una biblioteca compartida)
- UPDATE LIBRARY (Actualizar una biblioteca VTL)

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

 Sistemas operativos Windows

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los mandatos DEFINE LIBRARY y UPDATE LIBRARY. Con este parámetro se evita tener que etiquetar previamente un conjunto de cintas. También es más eficaz que utilizar el mandato LABEL LIBVOLUME, para lo que es necesario montar los volúmenes por separado. Si utiliza el parámetro AUTOLABEL, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows porque IBM Spectrum Protect no proporciona programas de utilidad para formatear o etiquetar estos tipos de soporte. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el mandato label.

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE LIBRARY

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY DRIVE	Muestra información sobre las unidades.

Mandato	Descripción
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE PATH	Cambia los atributos asociados con una ruta.

UPDATE LIBRARY (Actualizar una biblioteca 349X)

Utilice esta sintaxis para actualizar una biblioteca 349X.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRARY--nombre_biblioteca--+-----+----->
                                     '-SHARED-------Yes---'

>--+-----+----->
   '-RESETDrives-----+Yes-+-'
                                     '-No--'

>--+-----+----->
   '-AUTOLabel-----+No-----+-'
                                     +-Yes-----+
                                     '-OVERWRITE-'

>--+-----+-----><
   '-WORMSCatchcategory-----número-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

SHARED

Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes sólo si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

WORMSCatchcategory

Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables WORM en la biblioteca. Este parámetro es necesario si utiliza volúmenes WORM. Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo

pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca. Este parámetro sólo es válido cuando se utilizan volúmenes WORM 3592.

Restricción: Este parámetro sólo puede actualizarse si el parámetro WORM de la clase de dispositivo se establece en YES y WORMSCRATCHCATEGORY no tiene definido ningún valor actualmente.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

Sistemas operativos AIX Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

Sistemas operativos AIX Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

Ejemplo: añadir dispositivos nuevos a una biblioteca compartida

Actualizar una biblioteca 3494 compartida denominada 3494LIB2 con nuevos nombres de dispositivos. Sistemas operativos AIX

Sistemas operativos Linux

```
update library 3494lib2 device=/dev/lmcp1,/dev/lmcp2,/dev/lmcp3
```


Sistemas operativos Windows

```
update library 3494lib device=lb3.0.0.0,lb4.0.0.0,lb5.0.0.0
```

UPDATE LIBRARY (Actualizar una biblioteca ACSLS)

Utilice esta sintaxis para actualizar una biblioteca ACSLS.

Clase de privilegio

 Sistemas operativos Windows Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca--+-+-----+----->
                                     '-SHAREd--=====Yes---'

>--+-+-----+----->
   '-RESEtDrives--+-+Yes-+-'
                                     '-No--'

>--+-+-----+-----+-----+-----><
   '-AUTOLabel---+-+No-----+-'   '-ACSID---número-'
                                     +-+Yes-----+
                                     '-OVERWRITE-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.



SHAREd


Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHAREd=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESEtDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

ACSID (Obligatorio)

Especifica el número de esta biblioteca StorageTek que ha asignado el ACSSA (Automatic Cartridge System System Administrator). Puede ser un número del 0 al 126. Emita QUERY ACS en el sistema para obtener el número del identificador de la biblioteca. Este parámetro es necesario.

Consulte la documentación de StorageTek para obtener más información.

Ejemplo: actualizar un número de ID para una biblioteca ACSLS

Actualizar una biblioteca ACSLS denominada ACSLSLIB con un nuevo número de identificación.

```
update library acslslib acsid=1
```

UPDATE LIBRARY (Actualizar una biblioteca EXTERNAL)

Utilice esta sintaxis para actualizar una biblioteca externa.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca----->
```

```
>--+-----+-----<
```

```
'-AUTOLabel-----No-----'
```

```
+--Yes-----+
'-OVERWRITE-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

AUTOlabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

Ejemplo: actualizar un nombre de ruta para una biblioteca externa

Actualizar una biblioteca externa denominada EXTLIB con un nuevo nombre de ruta para el gestor de medios.

 Sistemas operativos AIX  Sistemas operativos Linux

```
update library extlib externalmanager=/v/server/mediamanager
```

 Sistemas operativos Windows

```
update library extlib externalmanager=c:\server\mediamanager
```

UPDATE LIBRARY (Actualizar una biblioteca FILE)

Utilice esta sintaxis para actualizar una biblioteca FILE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca--+-+-----+----><
                                     '-SHARed-------Yes----'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

SHAREd

Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

Ejemplo: actualizar una biblioteca FILE que se va a compartir

Actualice una biblioteca denominada FILE2 para que se pueda compartir:

```
update library file2 shared=yes
```

UPDATE LIBRARY (Actualizar una biblioteca manual)

Utilice esta sintaxis para actualizar una biblioteca manual.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca----->
>+-----+----->
  '-RESETDrives-----+Yes-+-'
                        '-No--'
>+-----+-----<
  '-AUTOLabel-----+No-----+-'
                        +-Yes-----+
                        '-OVERWRITE-'
```

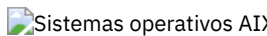
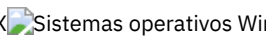
Parámetros

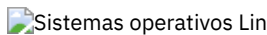
nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

UPDATE LIBRARY (Actualizar una biblioteca SCSI)

Utilice esta sintaxis para actualizar una biblioteca SCSI.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca----->
>---LIBType-----+SCSI-+-----+-----+----->
           '-VTL--'      '-SHARed-----Yes---'
>+-----+-----+-----+----->
   '-RESEtDrives-----+Yes-+-'
           '-No--'
>+-----+-----+-----+----->
   '-AUTOLabel-----+No-----+-'
           +-Yes-----+
           '-OVERWRITE-'
>+-----+-----+-----+----->
   '-RELABELSCRatch-----+No---+'
           '-Yes-'
>+-----+-----+-----+-----<
   '-SERial-----+núméro_serie-+-'
           '-AUTODetect---'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

LIBType (Obligatorio)

Especifica el tipo de biblioteca al que desea actualizar. Los valores posibles son:

VTL

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual SCSI.

Nota: Si selecciona la biblioteca VTL, se supone que se cumplen las siguientes condiciones:

- El entorno no incluye medios mixtos
- Hay rutas definidas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento, que utilizan la biblioteca

Si no se cumplen ambas condiciones, el rendimiento puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad cuando se utiliza la mayoría de unidades de forma simultánea.

SCSI

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual VTL.

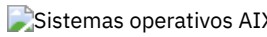
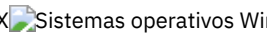
SHARED

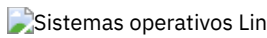
Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.
El dispositivo de biblioteca está conectado al dispositivo NAS, NDMP (protocolo de gestión de datos de red) accede indirectamente a él, y a las unidades de cintas solo se accede desde el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

SERIAL

Especifica el número de serie de la biblioteca que está actualizándose. Este parámetro es opcional. Los valores posibles son:

número_serie

Especifica el número de serie de la biblioteca que está actualizándose.

Si ya se ha definido una ruta para esta biblioteca, el número que especifica aquí se compara con el número que IBM Spectrum Protect ha detectado. Si los números no coinciden, el mandato no se ejecuta correctamente. Si no se ha definido una ruta, este número de serie se verifica cuando se defina una ruta.

AUTODetect

Especifica que, si ya se ha definido una ruta para esta biblioteca, IBM Spectrum Protect detecta y utiliza automáticamente el número de serie.

Si no se ha definido una ruta para esta biblioteca, el número de serie no se detecta.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando este parámetro se define con el valor SÍ, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta de volumen existente. Este parámetro es opcional y está pensado para utilizarse con una biblioteca de cintas virtual (VTL).

Nota: Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede afectar al rendimiento.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

UPDATE LIBRARY (Actualizar una biblioteca compartida)

Utilice esta sintaxis para actualizar una biblioteca compartida.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca----->
```

```
>--PRIMarylibmanager---nombre_servidor-----><
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

PRIMarylibmanager

Especifica el nombre del servidor responsable del control del acceso a los recursos de biblioteca. Debe definir este servidor con el mandato DEFINE SERVER para poder utilizarlo como gestor de bibliotecas.

Ejemplo: cambiar el servidor del gestor de bibliotecas para una biblioteca

Para un servidor de clientes de bibliotecas, cambiar el nombre del servidor gestor de bibliotecas por CASTOR.

```
update library ltolib primarylibmanager=castor
```

UPDATE LIBRARY (Actualizar una biblioteca VTL)

Utilice esta sintaxis para actualizar una biblioteca que está definida como VTL.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBRARY--nombre_biblioteca----->
>---LIBType---+VTL--+-----+----->
           '-SCSI-'      '-SHARED-----Yes---'
>+-----+----->
   '-RESETDrives-----+Yes+-'
                   '-No--'
>+-----+----->
   '-AUTOLabel-----+No-----+'
                   +-Yes-----+
                   '-OVERWRITE-'
>+-----+----->
   '-RELABELSCRatch-----+No--+-'
                   '-Yes-'
>+-----+-----<
   '-SERial-----+número_serie+-'
                   '-AUTODetect---'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType (Obligatorio)

Especifica el tipo de la biblioteca que está definiendo. Los valores posibles son:

SCSI

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual VTL.

VTL

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual SCSI.

Nota: Seleccione el tipo de biblioteca VTL solamente si se cumplen las condiciones siguientes:

- El entorno no incluye medios mixtos
- Hay rutas definidas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento, que utilizan la biblioteca

Si no se cumplen ambas condiciones, el rendimiento puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad cuando se utiliza la mayoría de unidades de forma simultánea.

SHARED

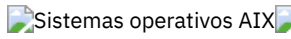

Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es


necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el mandato CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando se establece este parámetro en YES, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta del volumen existente.

Nota: Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede afectar al rendimiento.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

SERial

Especifica el número de serie de la biblioteca que está actualizándose. Este parámetro es opcional. Los valores posibles son:

número_serie

Especifica el número de serie de la biblioteca que está actualizándose.

Si ya se ha definido una ruta para esta biblioteca, el número que especifica aquí se compara con el número que IBM Spectrum Protect ha detectado. Si los números no coinciden, el mandato no se ejecuta correctamente. Si no se ha definido una ruta, este número de serie se verifica cuando se defina una ruta.

AUTODetect

Especifica que, si ya se ha definido una ruta para esta biblioteca, IBM Spectrum Protect detecta y utiliza automáticamente el número de serie.

Si no se ha definido una ruta para esta biblioteca, el número de serie no se detecta.

UPDATE LIBVOLUME (Cambiar el estado de un volumen de almacenamiento)

Utilice este mandato para cambiar el estado de un volumen de almacenamiento de acceso secuencial de una biblioteca.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate LIBVolume--nombre_biblioteca--nombre_volumen--STATus---+PRivate+-->
                                     '-SCRatch-'
>--+-----+-----<
   '-OWNer---nombre_servidor-'
```

Parámetros

nombre_biblioteca (Necesario)

Especifica el nombre de la biblioteca.

nombre_volumen (Necesario)

Especifica el nombre de volumen del volumen de almacenamiento.

STATus (Obligatorio)

Especifica un cambio del estado de un volumen de almacenamiento. Los valores posibles son los siguientes:




PRivate




Especifica que el servidor actualiza el volumen de almacenamiento a un volumen privado.

SCRatch

Especifica que el servidor actualiza el volumen de almacenamiento a un volumen reutilizable.

Restricción: No puede cambiar el estado de un volumen de privado a reutilizable si el volumen pertenece a una agrupación de almacenamiento o se define en el archivo histórico de volúmenes. Puede cambiar el estado si comete un error al dar de alta a los volúmenes en la biblioteca y asignar a los volúmenes el estado incorrecto.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica qué servidor es el propietario de un volumen privado en una biblioteca compartida en una SAN. Puede cambiar el propietario de un volumen privado en una biblioteca compartida (SAN) si emite el mandato desde el servidor gestor de bibliotecas. Si no especifica este parámetro, el servidor gestor de bibliotecas será el propietario del volumen privado.

Importante: No utilice OWNER como valor para volúmenes reutilizables. Sin embargo, puede utilizar OWNER al cambiar un volumen reutilizable a privado.







Ejemplo: actualizar el estado de un volumen

Actualice el volumen denominado WPDV00 de la biblioteca denominada AUTO de modo que refleje un estado de Privado (PRIVATE).

```
update libvolume auto wpdv00 status=private
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE LIBVOLUME

Mandato	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows LABEL LIBVOLUME	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.

UPDATE MACHINE (Actualizar información de máquina)

Utilice este mandato para actualizar la información de la máquina. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate MACHine--machine_name----->
>--+-----+-----+-----+----->
  '-DESCRiption----descripci3n-'  '-BUilding----edificio-'
>--+-----+-----+-----+----->
  '-FLoor----planta-'  '-ROom----sala-'
>--+-----+-----+-----+-----<<
  '-PRIority----n3mero-'  '-ADSMServer----+Yes+-'
                               '-No--'
```

Parámetros

nombre_máquina (Obligatorio)

Especifica el nombre de la máquina que se ha de actualizar.

DESCRiption

Especifica la descripción de la máquina. Este parámetro es opcional. El texto puede tener hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

BUilding

Especifica el nombre o número del edificio donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

FLoor

Especifica el nombre o número de la planta donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

ROom

Especifica el nombre o número de la sala donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

PRIority

Especifica la prioridad de restauración de la máquina en forma de un entero del 1 al 99. La prioridad más alta es 1. Este parámetro es opcional. Utilice este valor para determinar la prioridad de la recuperación de la máquina de cliente.

ADSMServer

Especifica si la máquina contiene un servidor de IBM Spectrum Protect. Este parámetro es opcional. Los valores posibles son:

No

Esta máquina no contiene un servidor de IBM Spectrum Protect.

Yes

Esta máquina contiene un servidor de IBM Spectrum Protect. Solo puede definirse una máquina que contenga un servidor de IBM Spectrum Protect.

Ejemplo: actualizar la información de una máquina específica

Actualizar la información de la máquina DISTRICT5 de modo que refleje que contiene el servidor.

```
update machine district5 admsserver=yes
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE MACHINE

Mandato	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.

UPDATE MGMTCLASS (Actualizar una clase de gestión)

Utilice este mandato para cambiar una clase de gestión. Para que los clientes puedan utilizar la clase de gestión actualizada, debe activar el juego de políticas que contiene la clase de gestión.

Importante: El mandato UPDATE MGMTCLASS no se ejecutará correctamente si se especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-UPDate MGMTclass----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+----->
  '-SPACEMGTEchnique---+--AUTOMatic-+-'
                        +-SElective-+
                        '-NONE-----'
>--+-----+----->
  '-AUTOMIGNonuse---días-'
>--+-----+----->
  '-MIGREQUIRESBkup---+--Yes-+-'
                        '-No--'
>--+-----+----->
  '-MIGDESTination---nombre_agrupación-'
>--+-----+-----<
```

'-DESCRiption----descripción-'

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas al que pertenece la clase de gestión. No puede actualizar una clase de gestión que pertenezca al juego de políticas ACTIVE.

nom_clase (Necesario)

Especifica la clase de gestión que se actualiza.

SPACEMGTEchnique

Especifica si un archivo que utiliza esta clase de gestión se puede seleccionar para una operación de migración. Este parámetro es opcional. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

AUTOMATIC

Especifica que se puede seleccionar el archivo para la migración automática y para la migración selectiva.

SElective

Especifica que el archivo se puede seleccionar únicamente para la migración selectiva.

NONE

Especifica que el archivo no se puede seleccionar para la operación de migración.

AUTOMIGNonuse

Especifica el número de días que deben transcurrir desde que se utilizó por última vez un archivo hasta que pueda seleccionarse para la migración automática. Este parámetro es opcional. Si SPACEMGTECHNIQUE no es AUTOMATIC, el servidor no tiene en cuenta este atributo. Puede especificar un entero de 0 a 9999.

Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

MIGREQUIRESBkup

Especifica si debe existir una versión de copia de seguridad de un archivo antes de que pueda migrarse un archivo. Este parámetro es opcional. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

Yes

Especifica que debe existir una versión de copia de seguridad.

No

Especifica que la versión de copia de seguridad es opcional.

MIGDESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los archivos migrados mediante clientes IBM Spectrum Protect for Space Management. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

El mandato no se ejecutará si especifica una agrupación de almacenamiento de copia como destino.

DESCRiption

Especifica una descripción de la clase de gestión. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("").

Ejemplo: actualizar el dominio de políticas y la agrupación de almacenamiento para una clase de gestión específica

Para la clase de gestión ACTIVEFILES, del juego de políticas VACATION del dominio de políticas EMPLOYEE_RECORDS, cambiar la agrupación de almacenamiento donde se almacenan los archivos migrados.

```
update mgmtclass employee_records vacation
activefiles migdestination=diskpool2
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE MGMTCLASS

Mandato	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

UPDATE NODE (Actualizar atributos del nodo)

Utilice este mandato para modificar los atributos de un nodo inscrito.

Debe utilizar el mandato RENAME NODE para cambiar el nombre de un nodo registrado.

Si actualiza el método de autenticación del nodo o el valor SSLREQUIRED del nodo y hay un administrador con el mismo nombre, cambie esos valores del ID de administrador.

Debe tener autorización de nivel de sistema para actualizar el método de autenticación del nodo o el valor SSLREQUIRED del nodo y también actualizar un ID de administrador con el mismo nombre. Si el administrador con el mismo nombre tiene la autorización de propietario de cliente sobre el nodo que se está actualizando, entonces no es necesaria la autorización de nivel de sistema. Debe tener privilegio de política sin restricciones o privilegio de política con restricciones para el dominio de políticas al que pertenece el nodo cliente.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Si cambia el modo de autenticación a LDAP y el nombre de nodo coincide con un ID de usuario de administración, podría darse un comportamiento imprevisto si se produce un cambio automático de contraseñas, ya que es posible que la contraseña se actualice dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

Cuando se registra o actualiza un nodo, puede especificar si los archivos dañados en el nodo pueden recuperarse de un servidor de réplica de destino. Los archivos sólo se pueden recuperar si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores de los parámetros a la recuperación de archivos dañados y replicados.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	No especificado	NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el nodo cliente.

Sintaxis

```

(1)
>>-UPDate Node-----nombre_nodo----->

>+-----+-----+-----+-----+----->
| (2)                                     |
+-----password--+-----+-----+-----+-----+
|                   '-FORCEPwreset--++-No--+-' |
|                   '-Yes-'                |
| '-FORCEPwreset----Yes-----'          |

>+-----+-----+-----+-----+----->
'-PASSExp----días-' '-CLOptset----option_set_name-'

>+-----+-----+-----+-----+----->
'-CONTACT----texto-' '-DOMAIN----domain_name-'

>+-----+-----+-----+-----+----->
'-COMPression--++-Client+-' '-ARCHDElete--++-Yes+-'
      +-Yes-----+                '-No--'
      '-No-----'

>+-----+-----+-----+-----+----->
'-BACKDElete--++-No--+-'
      '-Yes-'

>+-----+-----+-----+-----+----->
'-WHEREDomain----domain_name-'

>+-----+-----+-----+-----+----->

```

```

'-WHEREPlatform-----nombre_plataforma_cliente-'
>+-----+-----+-----+-----+-----+----->
'-MAXNUMMPP-----number-' '-KEEPMP-----+No--+-'
                               '-Yes-'
>+-----+-----+-----+-----+-----+----->
'-URL-----dirección_url-' '-UTILITYUrl-----utility_url-'
                               (3)
>+-----+-----+-----+-----+-----+----->
'-AUTOFSRename-----+Yes-----+'
                               +-No-----+
                               '-Client-'
>+-----+-----+-----+-----+-----+----->
'-VALIdateprotocol-----+No-----+-'
                               +-Dataonly-+
                               '-All-----'
>+-----+-----+-----+-----+-----+----->
'-TXNGroupmax-----+0-----+-'
                               '-número-'
.-DATAWritepath-----ANY-----
>+-----+-----+-----+-----+-----+----->
'-DATAWritepath-----+ANY-----+'
                               +-LAN-----+
                               '-LANFree-'
.-DATAReadpath-----ANY-----
>+-----+-----+-----+-----+-----+----->
'-DATAReadpath-----+ANY-----+'
                               +-LAN-----+
                               '-LANFree-'
>+-----+-----+-----+-----+-----+----->
'-TARGETLevel-----V.R.M.F-'
.-SESSIONINITiation-----Clientorserver-----
>+-----+-----+-----+-----+-----+-----+----->
'-SESSIONINITiation-----+Clientorserver-----+'
                               |
                               '-SERVEROnly--HLAddress----dirección_ip--LAddress----puerto_tcp-----' (4) |
>+-----+-----+-----+-----+-----+----->
'-HLAddress----ip_address-'
>+-----+-----+-----+-----+-----+----->
|                               (4) |
'-LAddress----puerto_tcp-----'
>+-----+-----+-----+-----+-----+----->
'-EMAILAddress----ID_usuario@nodo-'
>+-----+-----+-----+-----+-----+----->
'-DEDUPlication-----+SERVEROnly-----+'
                               '-Clientorserver-'
>+-----+-----+-----+-----+-----+----->
|                               (5) |
'-BACKUPINITiation-----+All--+-----+'
                               '-ROOT-'
>+-----+-----+-----+-----+-----+----->
'-BKREPLRuledefault-----+ALL_DATA-----+'
                               +-ACTIVE_DATA-----+
                               +-ALL_DATA_HIGH_PRIORITY-----+
                               +-ACTIVE_DATA_HIGH_PRIORITY-+
                               +-DEFAULT-----+
                               '-NONE-----'
>+-----+-----+-----+-----+-----+----->
'-ARREPLRuledefault-----+ALL_DATA-----+'
                               +-ALL_DATA_HIGH_PRIORITY-+
                               +-DEFAULT-----+
                               '-NONE-----'

```

```

>----->
'-SPREPLRuledefault-----+ALL_DATA-----+'
      +-ALL_DATA_HIGH_PRIORITY--+
      +-DEFAULT-----+
      '-NONE-----'

>----->
|                                     |
|           (6)                       |
| '-REPLState-----+ENabled--+-----+' |
|          '-DISabled-' |                                     |
|                                     | (7) |
|                                     | '-REPLMode-----+--SYNCSEnd-----+' |
|                                     |          '-SYNCRECeive-' |

>----->
'-RECOVERDamaged-----+Yes--+-'
      '-No--'

>----->
'-ROLEOVERRIDE-----+Client-----+'
      +-Server-----+
      +-Other-----+
      '-Usereported-'

>----->
|                                     |
|                                     | (8) |
|                                     | .-SYNCLdapdelete-----+--No--. |
|                                     | |
| '-AUTHentication-----+Local--+-----+' |
|          '-LDap--'   | '-SYNCLdapdelete-----+Yes--+-' |
|                                     |          '-No--' |

(9)
>----->
'-SSLrequired-----+Yes-----+'
      +-No-----+
      +-Default----+
      '-SERVERonly-'

.-SESSIONSECurity-----TRANSitional-----.

>----->
'-SESSIONSECurity-----+STRict-----+'
      '-TRANSitional-'

.-SPLITLARGEObjects-----Yes-----.

>----->
'-SPLITLARGEObjects-----+Yes--+-'
      '-No--'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.
2. Las contraseñas son opcionales para este mandato, excepto si se cambia el método de autenticación de LDAP a LOCAL.
3. El parámetro VALIDATEPROTOCOL está en desuso.
4. HLADDRESS y LLADDRESS se deben establecer o especificar previamente en el mandato UPDATE NODE o REGISTER NODE para utilizar SESSIONINITIATION=SERVERONLY.
5. El parámetro BACKUPINITIATION se ignora si el sistema operativo del nodo cliente no está soportado.
6. Si especifica el parámetro REPLSTATE y no especifica el parámetro REPLMODE, la modalidad de réplica del nodo se establece en SEND.
7. Si especifica el parámetro REPLMODE, también debe especificar el parámetro REPLSTATE.
8. El parámetro SYNCLDAPDELETE se aplica solamente si un nodo que se autentica en un servidor Lightweight Directory Access Protocol (LDAP) vuelve a la autenticación local.
9. El parámetro SSLREQUIRED está en desuso.

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se ha de actualizar. Puede utilizar caracteres comodín para especificar este nombre.

Restricción: Al actualizar una contraseña con el mandato UPDATE NODE, no puede utilizar un carácter comodín con el parámetro

node_name.

contraseña

Especifica la nueva contraseña del nodo cliente. Este parámetro es opcional en la mayoría de los casos. Si se cambia el método de autenticación de LDAP a local, es necesaria una contraseña. Si el método de autenticación de nodos es LDAP, no especifique ninguna contraseña utilizando el mandato UPDATE NODE. La longitud máxima de la contraseña es de 64 caracteres. Las contraseñas continúan siendo actuales durante un período de tiempo que queda determinado por el período de caducidad de contraseñas.

FORCEPwreset

Especifica si se forzará que un cliente cambie o restablezca la contraseña. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el período de caducidad de contraseña se establece mediante el mandato SET PASSEXP. No se fuerza que un cliente cambie o restablezca la contraseña mientras se intenta iniciar la sesión en el servidor.

Yes

Especifica que la contraseña del administrador o del nodo de cliente caducará durante la próxima conexión. El cliente debe cambiar o restaurar la contraseña en el próximo inicio de sesión.

Restricciones:

- En el caso de los nodos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizan los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si tiene previsto especificar AUTHENTICATION=LDAP.
- Si tiene previsto actualizar un nodo para la autenticación con un servidor LDAP y ha especificado FORCEPWRESET=YES, debe cambiar la contraseña para poder especificar FORCEPWRESET=NO y AUTHENTICATION=LDAP.

PASSExp

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña en el rango de 0 – 9999 días. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, el período de caducidad de contraseña permanece igual.

Puede cambiar el período de caducidad de la contraseña mediante los mandatos UPDATE NODE o SET PASSEXP. Para establecer un período de caducidad común para todos los administradores y nodos cliente, emita el mandato SET PASSEXP. También puede utilizar el mandato SET PASSEXP para establecer períodos de caducidad de contraseña de forma selectiva. Si establece un período de caducidad de la contraseña de forma selectiva mediante el mandato REGISTER NODE, el mandato UPDATE NODE o el mandato SET PASSEXP, el período de caducidad se excluirá de los períodos de caducidad de contraseñas comunes que se han creado mediante el mandato SET PASSEXP.

Puede utilizar el mandato RESET PASSEXP para restablecer el período de caducidad de contraseñas en un período de caducidad común. Este parámetro no se aplica a las contraseñas que se autentican con un servidor de directorios LDAP.

CLOptset

Especifica el nombre del conjunto de opciones que ha de utilizar el cliente. Este parámetro es opcional. Para eliminar el conjunto de opciones de cliente, especifique el parámetro CLOPTSET con una serie vacía ("").

CONtact

Especifica una serie de texto de información que identifica el nodo de cliente. Este parámetro es opcional. La longitud máxima de la serie de texto es de 255 caracteres. La información de contacto debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir la información de contacto definida, especifique una serie nula ("").

DOmain

Especifica el nombre del dominio de políticas en el que desea registrar el nodo cliente. Este parámetro es opcional.

Restricción: en el caso de los servidores que tienen la protección de retención de datos activada, un nodo inscrito archivado no se puede reasignar a un dominio de políticas diferente.

COMPrission

Especifica si el nodo de cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada. Este parámetro es opcional.

Restricción: Este parámetro no se puede especificar para un nodo NAS.

Puede especificar uno de los siguientes valores:

Client

Especifica que el cliente determina si se comprimirán los archivos.

Yes

Especifica si el nodo de cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada.

No

Especifica que el nodo de cliente no comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada.

ARCHDElete

Especifica si el nodo cliente puede suprimir sus propias copias archivadas del servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Yes

Especifica que el nodo cliente puede suprimir sus propias copias archivadas del servidor.

No

Especifica que el nodo cliente no puede suprimir sus propias copias archivadas del servidor.

BACKDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el nodo cliente no puede suprimir sus propias copias de seguridad del servidor.

Yes

Especifica que el nodo cliente puede suprimir sus propias copias de seguridad del servidor.

WHEREDomain

Especifica el nombre del dominio de políticas que se ha de utilizar como filtro junto con el nombre de nodo para seleccionar los nodos que se actualizan. Este parámetro es opcional.

WHEREPlatform

Especifica el nombre de la plataforma de cliente que se ha de utilizar como filtro junto con el nombre de nodo para seleccionar los nodos que se actualizan. Este parámetro es opcional.

MAXNUMMP

Especifica el número máximo de puntos de montaje que puede utilizar un nodo en el servidor o en el agente de almacenamiento sólo para operaciones como la copia de seguridad, el archivado y la migración IBM Spectrum Protect for Space Management. El parámetro es opcional y no se aplica a los nodos con un tipo NAS o SERVER. El valor predeterminado es 1. Puede especificar un entero en el rango de 0 a 999. Un valor de 0 especifica que un nodo no puede adquirir ningún punto de montaje para una operación de almacenamiento de datos de cliente. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos las operaciones de almacenamiento de datos simultáneas del mismo nodo cliente, y puede que impidan que las operaciones de almacenamiento de datos obtengan puntos de montaje.

En el caso de los volúmenes de una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA, el servidor puede disponer, simultáneamente, de varias sesiones que lean y de un único proceso que grabe en el mismo volumen. Para aumentar la concurrencia y proporcionar un acceso eficiente para nodos que tienen datos en agrupaciones de almacenamiento FILE o CENTERA, incremente el valor del parámetro MAXNUMMP.

En nodos que almacenan datos en agrupaciones de almacenamiento primarias con la función de grabación simultánea activada, deberá ajustar el valor del parámetro MAXNUMMP para especificar el número correcto de puntos de montaje de cada sesión de cliente. Una sesión de cliente requiere un punto de montaje para la agrupación de almacenamiento primario y un punto de montaje para cada agrupación de almacenamiento de copias y cada agrupación de datos activos.

URL

Especifica el URL del cliente web de IBM Spectrum Protect que se ha configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

Este parámetro es opcional. El URL debe incluir el nombre DNS o la dirección IP del sistema cliente y el número de puerto que está definido en el sistema cliente para el cliente web de IBM Spectrum Protect. Por ejemplo, `http://client.mycorp.com:1581`

Si desea eliminar el valor de este parámetro, especifique comillas simples vacías o bien comillas dobles vacías, sin espacios (" para comillas simples o "" para comillas dobles).

UTILITYUrI

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde Centro de operaciones.

Este parámetro es opcional. Puede especificar un URL de hasta 200 caracteres de longitud. El URL debe empezar por `https`. Incluye el nombre DNS o la dirección IP del sistema cliente y el número de puerto que se ha definido en el sistema cliente para los servicios de gestión de cliente de IBM Spectrum Protect. Por ejemplo, `https://client.mycorp.com:9028`

Si se omite el número de puerto, el Centro de operaciones utiliza el número de puerto 9028, que es el número de puerto predeterminado cuando se instalan los servicios de gestión del cliente en el sistema cliente.

KEEPMP

Especifica si el nodo cliente mantiene el punto de montaje durante toda la sesión. El parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el nodo de cliente libera el punto de montaje durante la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se publicarán los puntos de montaje que mantenga la sesión.

Yes

Especifica que el nodo cliente debe retener el punto de montaje durante toda la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se retendrán los puntos de montaje que mantenga la sesión.

AUTOFSRename

Especifica si se solicita al cliente que redetermine los espacios de archivos cuando el sistema cliente se actualiza a un cliente que tiene soporte para Unicode. La solicitud y la redeterminación, si están permitidas, sólo se producen cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. La redeterminación cambia los nombres de los espacios de archivos de los que se ha hecho una copia de seguridad que no están en Unicode en el almacenamiento del servidor. A continuación, se realiza una copia de seguridad de los espacios de archivos en Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS X y NetWare.

Importante: Una vez que se ha instalado el cliente que admite Unicode, los nuevos espacios de archivos de los que el cliente hace una copia de seguridad se almacenan en el almacenamiento del servidor utilizando la página de códigos UTF-8. UTF-8 es un formato de codificación orientado a bytes que especifica el estándar de Unicode.

Puede especificar uno de los siguientes valores:

Yes

El servidor redetermina automáticamente los espacios de archivos existentes cuando el sistema cliente se actualiza en un cliente que tiene soporte para Unicode, y el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. La redeterminación se produce si el cliente utiliza una interfaz gráfica de usuario, la línea de mandatos o el planificador cliente.

Por ejemplo, el servidor redetermina una unidad del siguiente modo:

- Nombre original: D_DRIVE
- Nombre nuevo: D_DRIVE_OLD

El nombre nuevo indica que el espacio de archivos se almacena en el servidor en un formato que no es Unicode.

No

El servidor no redetermina automáticamente los espacios de archivos cuando el sistema cliente se actualiza en un cliente que tiene soporte para Unicode, y el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial.

Client

La opción AUTOFSRENAME en el archivo de opciones del cliente determina si los espacios de archivos están redeterminados.

De forma predeterminada, la opción de cliente se define en PROMPT. Cuando el sistema cliente se actualiza en un cliente compatible con Unicode y el cliente realiza una operación de IBM Spectrum Protect con la interfaz gráfica de usuario o la línea de mandatos, el programa pregunta una vez al usuario si desea cambiar el nombre los espacios de archivos.

Cuando el planificador cliente realiza una operación, el programa no ofrece ninguna solicitud sobre redeterminación y no redetermina los espacios de archivos. Las copias de seguridad de los espacios de archivos existentes se envían como antes (no en Unicode).

VALIDateprotocol (en desuso)

Especifica si IBM Spectrum Protect realiza una comprobación de redundancia cíclica para validar los datos enviados entre el cliente y el servidor. El parámetro es opcional.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2 y Tivoli Storage Manager Versión 7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

TXNGroupmax

Especifica el número máximo de archivos que se transferirán como un grupo entre un cliente y un servidor entres puntos de validación de transacciones. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.

Al especificar 0 se indica que el nodo utiliza el valor global del servidor establecido en el archivo de opciones del servidor. Si desea emplear un valor distinto del valor global del servidor, especifique un valor entre 4 y 65.000 para este parámetro. El valor del nodo prevalece sobre el valor del servidor.

Consejo: Si aumenta el valor de TXNGROUPMAX, aumenta la utilización de las anotaciones de recuperación. Una mayor utilización de las anotaciones de recuperación puede incrementar el riesgo de quedarse sin espacio de anotaciones. Evalúe el rendimiento de cada uno de los nodos antes de cambiar este parámetro.

DATAWritepath

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento tales como copia de seguridad o archivado. El parámetro es opcional. Recuerde: Si no hay disponible una ruta, el nodo no puede enviar ningún dato. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará.

Puede especificar uno de los siguientes valores:

ANY

Especifica que los datos se envían al servidor, agente de almacenamiento o a ambos mediante cualquier ruta disponible. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se mueven a través de la LAN.

LAN

Especifica que los datos se envían a través de la LAN.

LANFree

Especifica que los datos se envían a través de una ruta fuera de la LAN.

DATAReadpath

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. El parámetro es opcional.

Recuerde: Si no hay disponible una ruta, no es posible leer datos. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará. El valor de la vía de acceso de transferencia también se aplica a las conexiones de migración tras error. Si el valor se establece en LANFree, puede producirse la migración tras error para el nodo en el servidor secundario.

Puede especificar uno de los siguientes valores:

ANY

Especifica que el servidor, agente de almacenamiento o ambos utilizan cualquier ruta disponible para leer datos. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se leen a través de la LAN.

LAN

Especifica que los datos se leen a través de la LAN.

LANFree

Especifica que los datos se leen utilizando una ruta fuera de la LAN.

SESSIONINITiation

Controla si el servidor o el cliente ha de iniciar las sesiones. El parámetro es opcional.

Clientorserver

Especifica que el cliente puede iniciar sesiones con el servidor comunicándose en el puerto TCP/IP que se ha definido con la opción TCPPOINT. También puede utilizarse la planificación por petición de servidor para solicitar al cliente que se conecte con el servidor.

SERVEROnly

Especifica que el servidor no acepta peticiones de sesiones del cliente. Todas las sesiones deberá iniciarlas la planificación por petición de servidor en el puerto que se ha definido para el cliente con los mandatos REGISTER o UPDATE NODE. No se puede utilizar Client Acceptor, dsmscad, para iniciar el planificador si SESSIONINITIATION está establecido en SERVERONLY.

HAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente

establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

HLAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro opcional sólo se utiliza cuando se define SESSIONINITIATION con el valor SERVERONLY, independientemente de las direcciones que el cliente haya utilizado anteriormente para contactar con el servidor. Si SESSIONINITIATION SERVERONLY no está en uso, la opción no tendrá ningún efecto.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro opcional sólo se utiliza cuando se define SESSIONINITIATION con el valor SERVERONLY, independientemente de las direcciones que el cliente haya utilizado anteriormente para contactar con el servidor. Si SESSIONINITIATION SERVERONLY no está en uso, la opción no tendrá ningún efecto.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

EMAILAddress

Este parámetro se utiliza para obtener más información de contacto. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

DEDUPlication

Especifica dónde puede producirse la eliminación de datos duplicados para este nodo. Puede especificar uno de los siguientes valores:

SERVEROnly

Especifica que los datos almacenados por este nodo sólo se pueden desduplicar en el servidor.

Clientorserver

Indica que los datos almacenados por este nodo se pueden desduplicar en el cliente o en el servidor. Para realizar la eliminación de datos duplicados en el cliente, debe especificar el valor YES en la opción de cliente DEDUPLICATION. Puede especificar esta opción en el archivo de opciones del cliente o en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

TARGETLevel

Especifica el paquete de despliegue del cliente que se utiliza este nodo. Puede sustituir por un paquete de release aplicable V.R.M.F (Version.Release.Modification.Fix) Level. Por ejemplo: TARGETLevel=6.2.0.0.

Debe especificar cada segmento con un número aplicable a un paquete de despliegue. No se puede utilizar el asterisco en ningún campo como sustituto de un número válido. Para suprimir un valor existente, especifique una serie nula (" "). El parámetro es opcional.

Restricción: El parámetro TARGETLEVEL no se aplica a los nodos con un tipo NAS o SERVER.

BACKUPINITiation

Especifica si el ID de usuario no root en el nodo de cliente puede realizar una copia de seguridad de los archivos en el servidor. El parámetro es opcional. El valor predeterminado es ALL, que indica que los ID de usuario no root pueden realizar una copia de seguridad de los datos en el servidor. Puede seleccionar uno de los siguientes valores:

All

Especifica que los ID de usuario no root pueden realizar una copia de seguridad de los archivos en el servidor. ALL es el valor predeterminado si no se especifica BACKUPINITIATION.

ROOT

Especifica que sólo el ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor.
Restricción: El servidor ignora el atributo si el cliente de archivado y copia de seguridad se conecta desde un sistema operativo distinto de AIX, Linux, Solaris o Mac OS.

BKREPLRuledefault, ARREPLRuledefault, y SPREPLRuledefault

Especifica la regla de réplica que se aplica a un tipo de datos si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT:

BKREPLRuledefault

Especifica la regla de réplica de los datos de copia de seguridad.

ARREPLRuledefault

Especifica la regla de réplica de los datos de archivado.

SPREPLRuledefault

Especifica la regla de réplica de los datos gestionados por espacio.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que un nodo cliente contiene datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a ambos tipos de datos, especifique `BKREPLRULEDEFAULT=ACTIVE_DATA_HIGH_PRIORITY` `ARREPLRULEDEFAULT=ALL_DATA`.

Puede especificar las siguientes reglas:

ALL_DATA

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad normal.

ACTIVE_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal. Esta regla sólo es válida para BKREPLRULEDEFAULT.

Atención:

Si especifica ACTIVE_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando se instala una versión anterior a la Versión 7.1.1 en los servidores de réplica de origen o de destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCE_RECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la duplicación, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino de una versión anterior a V7.1.1.

Si las condiciones anteriores no son verdaderas, se duplican todos los archivos nuevos y cambiados desde la última réplica, incluidos los archivos inactivos, y los archivos se suprimen cuando caducan.

ALL_DATA_HIGH_PRIORITY

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad alta.

ACTIVE_DATA_HIGH_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE_DATA excepto que los datos se replican con una prioridad alta. Esta regla sólo es válida para BKREPLRULEDEFAULT.

DEFAULT

Replica los datos según la regla de réplica del servidor para los datos de copia de seguridad.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es especificar `ARREPLRULEDEFAULT=DEFAULT`. Asegúrese de que las reglas de espacio de archivos de los datos de archivado también se establezcan en DEFAULT y que la regla del servidor de los datos de archivado se establezca en ALL_DATA_HIGH_PRIORITY.

Restricción: Si se configura un nodo para la réplica, las reglas de espacio de archivos se establecen en DEFAULT después de que el nodo almacene datos en el servidor de réplica de origen.

NONE

Los datos del tipo especificado no se replican.

Por ejemplo, si no desea replicar los datos gestionados por espacio que pertenecen a un nodo de cliente, especifique `SPREPLRULEDEFAULT=NONE`

REPLState

Especifica si los datos que pertenecen al nodo de cliente están preparados para replicarse. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

ENabled

Especifica que el nodo de cliente está preparado para la réplica.

DISabled

Especifica que la réplica no se realiza hasta que la activa.

La respuesta del sistema a estos valores depende de los siguientes factores:

Si la definición de nodo de cliente existe sólo en el servidor de réplica de origen y está configurando el nodo de cliente para la réplica por primera vez

Si establece el estado de réplica en `ENABLED` o `DISABLED`, la modalidad de réplica del nodo en el servidor de réplica de origen se establece automáticamente en `SEND` después de que se emita el mandato `UPDATE NODE`. Cuando se realiza la réplica por primera vez, se crea automáticamente una definición de nodo de cliente en el servidor de destino. El estado de réplica del nodo de cliente en el servidor de destino se establece automáticamente en `ENABLED`. La modalidad de réplica se establece en `RECEIVE`.

Si la definición de nodo de cliente existe en los servidores de réplica de origen y destino, y los datos del nodo se han replicado previamente.

Para que se produzca la réplica, el estado de réplica del nodo de cliente en los servidores de origen y destino debe establecerse en `ENABLED`. Por ejemplo, si el estado de réplica de un nodo de cliente en el servidor de origen es `ENABLED` y el estado de réplica en el servidor de destino es `DISABLED`, la réplica no se realiza.

Si la definición de nodo de cliente existe en los servidores de réplica de origen y destino, y los datos del nodo se han exportado previamente desde el servidor de réplica de origen y se han importado al servidor de réplica de destino.

En este caso, está configurando los nodos de cliente para sincronizar los datos entre los dos servidores. Cuando se realiza la réplica por primera vez, el estado de réplica del nodo de cliente en el servidor de destino se establece automáticamente en `ENABLED`. Los datos en los servidores de origen y destino se sincronizan.

Restricción: Para sincronizar los datos, debe especificar el parámetro `REPLMODE` además del parámetro `REPLSTATE`.

Puede especificar el parámetro `REPLMODE` solo si nunca se ha replicado el nodo de cliente:

- Si la definición de nodo de cliente sólo existe en el servidor de réplica de origen, la modalidad de réplica del nodo en el servidor de réplica de origen se establece automáticamente en `SEND` cuando se emite el mandato `UPDATE NODE`. La modalidad de réplica del nodo en el servidor de réplica de destino se establece automáticamente en `RECEIVE`.
- Si los datos que pertenecen al nodo se han replicado previamente, la modalidad de réplica del nodo en el servidor de réplica de origen es `SEND`. La modalidad de réplica del nodo en el servidor de réplica de destino es `RECEIVE`.

REPLMode

Especifica si se deben sincronizar los datos que pertenecen a este nodo de cliente. Especifique este parámetro sólo si los datos que pertenecen al nodo de cliente se han exportado desde el servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

Para sincronizar los datos, debe emitir el mandato `UPDATE NODE` en los servidores de réplica de origen y destino, y especificar los parámetros `REPLMODE` y `REPLSTATE`. El valor que especifica para el parámetro `REPLMODE` depende de si el servidor es un origen o un destino de los datos replicados.

Puede especificar uno de los siguientes valores:

SYNCSEnd

Especifica que los datos que pertenecen a este nodo de cliente se sincronizan con los datos en un servidor de destino durante la réplica. Especifique este valor sólo en el servidor que ha exportado los datos. Cuando la sincronización finaliza, la modalidad de réplica del nodo de cliente en el servidor de origen se establece automáticamente en `SEND`. La modalidad de réplica permanece en `SEND` a no ser que elimine el nodo emitiendo el mandato `REMOVE REPLNODE`.

SYNCRECeive

Especifica que los datos que pertenecen a este nodo de cliente se sincronizan con los datos en un servidor de origen durante la réplica. Especifique este valor sólo en el servidor que ha importado los datos. Cuando la sincronización finaliza, la modalidad de réplica del nodo de cliente en el servidor de destino se establece automáticamente en `RECEIVE`. La modalidad de réplica permanece en `RECEIVE` a no ser que elimine el nodo emitiendo el mandato `REMOVE REPLNODE`.

Restricciones:

- Puede establecer el parámetro REPLMODE solo si el estado de réplica inicial es NONE. Para sincronizar los datos, cambie el estado de réplica a ENABLED o DISABLED y especifique un valor para el parámetro REPLMODE.
- Los datos sólo pueden sincronizarse si especifica `DATES=ABSOLUTE` en el mandato `IMPORT NODE`. Si ha especificado `DATES=RELATIVE` para importar datos, debe renombrar el nodo o suprimir sus datos antes de realizar la réplica. Si no sigue una de estas indicaciones, puede perder datos.
- Si el parámetro REPLMODE se ha establecido incorrectamente, debe emitir el mandato `REMOVE REPLNODE` antes de actualizar la definición del nodo de cliente. Por ejemplo, supongamos que ha actualizado la definición de un nodo de cliente cuyos datos deseaba replicar. Los datos que pertenecen al nodo se han exportado previamente al servidor de réplica de destino. Ha especificado `ENABLED` como el valor del parámetro `REPLSTATE`. Sin embargo, no ha especificado `SYNCSEND` en el servidor de réplica de origen. Como resultado, el parámetro REPLMODE se ha establecido automáticamente en `SEND`, y los datos pertenecientes al nodo no se han podido sincronizar o replicar.

La emisión de `REMOVE REPLNODE` establece el estado de réplica y la modalidad de réplica en `NONE`. Cuando finalice el mandato `REMOVE REPLNODE`, vuelva a emitir el mandato `UPDATE NODE` con los valores y los parámetros correctos.

RECOVERDamaged

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino. El parámetro es opcional. El valor predeterminado es `YES`. Puede especificar uno de los siguientes valores:

Yes

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino está habilitada para este nodo.

No

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino no está habilitada para este nodo.

Consejo: El valor del parámetro `RECOVERDAMAGED` es sólo uno de varios valores que determinan si se recuperan los archivos dañados. Para obtener información sobre cómo especificar los valores, consulte Valores que afectan a la recuperación de archivos dañados.

ROLEOVERRIDE

Especifica si se debe alterar temporalmente el rol notificado del cliente para la creación de informes de estimación de unidades de valor de procesador (PVU). El valor predeterminado es `USERREPORTED`.

El rol notificado por el cliente es un dispositivo de cliente (por ejemplo, una estación de trabajo) o un dispositivo de servidor (por ejemplo, un servidor de archivos/impresión, un servidor de aplicaciones o una base de datos). De forma predeterminada, el cliente notifica su rol basándose en el tipo de cliente y el sistema operativo. Todos los clientes notifican inicialmente su rol como dispositivo de servidor, excepto los clientes de archivado y copia de seguridad de IBM Spectrum Protect que ejecutan distribuciones de estaciones de trabajo de Microsoft Windows (Windows Vista) y Macintosh OS X.

Especifique uno de los siguientes valores:

Client

Especifica un dispositivo de cliente.

Server

Especifica un dispositivo de servidor.

Otro

Especifica que este nodo no se va a utilizar para la creación de informes de estimaciones de PVU. El valor Otro es útil cuando se despliegan varios nodos para un sistema físico (por ejemplo, entornos virtuales, nodos de prueba, nodos retirados y nodos que no estén en producción ni en clúster).

Userreported

Utilice el rol notificado que proporciona el cliente.

AUTHentication

Este parámetro determina el método de autenticación de la contraseña que utiliza; LDAP o local.

Local

Especifica que el nodo utiliza la base de datos del servidor de IBM Spectrum Protect local para almacenar las contraseñas.

LDap

Especifica que el nodo utiliza un servidor de directorios LDAP para autenticar las contraseñas. Las contraseñas no se almacenan en la base de datos de IBM Spectrum Protect.

SYNClapdelete

Este parámetro solo se aplica si desea que un nodo que se autentica en un servidor de directorios LDAP (Lightweight Directory Access Protocol) pase a autenticarse con IBM Spectrum Protect. El parámetro especifica si se ha de eliminar el nodo del servidor LDAP.

Sí

Especifica que el nodo se elimina.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que el nodo no se elimina. Este es el valor predeterminado.

SSLrequired (en desuso)

Especifica si el nodo debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect . El parámetro es opcional. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red

Importante: A partir del software de IBM Spectrum Protect V8.1.2 y del software de Tivoli Storage Manager V7.1.8, este parámetro ha quedado en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

SESSIONSECURITY

Especifica si el nodo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRICT

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el nodo. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el nodo pueda autenticarse en el servidor:

- Tanto el nodo como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el nodo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el nodo.

Los nodos que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

TRANSITIONAL

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el nodo no cumplen nunca los requisitos para el valor STRICT, el nodo continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un nodo cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el nodo ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, el nodo ya no se puede autenticar con un protocolo menos seguro. Por ejemplo, si se actualiza un nodo que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, cuando el nodo se autentica en el servidor IBM Spectrum Protect como nodo de otro servidor.

SPLITLARGEObjects

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. Si se especifica Sí, el servidor divide los objetos grandes (más de 10 GB) en partes más pequeñas cuando se almacenan en un nodo de cliente. Si se especifica No, se ignora este proceso. Especifique No solo si lo que pretende es maximizar el rendimiento de las copias de seguridad directamente en la cinta. El valor predeterminado es Yes (sí).

Ejemplo: Actualice el nodo SIMON para que se autentique con un servidor de directorios LDAP y se conecte utilizando SSL

```
update node simon authentication=ldap sslrequired=yes
```

Cuando especifica el parámetro SSLREQUIRED, el servidor no se configura automáticamente para SSL. Debe seguir las instrucciones para conectarse a SSL para que el ejemplo funcione.

Ejemplo: Actualizar todos los nodos para comunicarse con un servidor utilizando la seguridad de sesión estricta.

Actualice todos los nodos para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
update node * sessionsecurity=strict
```

Ejemplo: actualizar un nodo con información de release de software para un futuro despliegue

La característica de despliegue de cliente permite actualizar un cliente de archivado y copia de seguridad a un nuevo release. La información que se genera a partir del mandato UPDATE NODE le ayudará cuando planifique un despliegue. La información se almacena para un futuro despliegue y puede verse emitiendo el mandato QUERY NODE. Después del despliegue, puede emitir el mandato QUERY NODE para ver el nivel actual y el nivel de destino. En este ejemplo, para actualizar el nodo LARRY al cliente de archivado y copia de seguridad versión 6.3.0.0.

```
update node LARRY targetlevel=6.3.0.0
```

Ejemplo: actualizar la copia de seguridad de un nodo para comprimir los datos e impedir que el cliente pueda suprimir copias archivadas

Actualice el nodo LARRY para que los datos del nodo LARRY se compriman cuando IBM Spectrum Protect realice la copia de seguridad o el archivado de éstos, de modo que el cliente no pueda suprimir las copias archivadas.

```
update node larry compression=yes archdelete=no
```

Ejemplo: actualizar el número de archivos de un nodo que pueden transferirse como grupo

Actualizar el nodo LARRY e incrementar el valor TXNGroupmax a 1.000.

```
update node larry txngroupmax=1000
```

Ejemplo: actualización de un nodo y optimización de almacenamiento en el cliente

Actualice un nodo BOB para que puedan eliminarse los duplicados en el cliente.

```
update node bob deduplication=clientorserver
```

Ejemplo: actualizar el rol del nodo BOB a un dispositivo de servidor para la creación de informes de estimación de PVU

Si desea acumular valores PVU, sólo se registran roles del dispositivo de servidor. Puede actualizar un nodo desde un dispositivo de cliente a un dispositivo de servidor emitiendo el mandato UPDATE NODE. En este ejemplo, el nodo BOB se actualiza a un dispositivo de servidor.

```
update node bob role=server
```

Ejemplo: actualizar una definición de nodo en un servidor de réplica de origen

NODE1 está definido en un servidor de réplica de origen. Los datos que pertenecen a NODE1 se han exportado previamente a un servidor de réplica de destino. Actualice la regla de réplica para los datos de copia de seguridad que pertenecen a NODE1, para que los datos de copia de seguridad activos se repliquen con una prioridad alta. Active la réplica para el nodo. Configure la sincronización de datos con el servidor de réplica de destino.

```
update node node1 bkreplruledefault=active_data_high_priority  
replstate=enabled replmode=syncsend
```

Ejemplo: actualizar una definición de nodo para habilitar la recuperación de archivos dañados

Actualizar el nodo PAYROLL para habilitar la recuperación de archivos dañados a partir de un servidor de réplica de destino.


```
update node payroll recoverdamaged=yes
```

Mandatos relacionados

Tabla 2. Mandatos relacionados con UPDATE NODE

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.
RENAME NODE	Cambia el nombre de un nodo cliente.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.

Referencia relacionada:

 Opción de cliente SSL

UPDATE NODEGROUP (Actualizar un grupo de nodos)

Utilice este mandato para modificar la descripción de un grupo de nodos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

Sintaxis

```
>>-UPDate NODEGroup--nombre_grupo----->
>--DESCRiption===--descripción-----><
```

Parámetros

nombre_grupo

Especifica el nombre del grupo de nodos cuya descripción desea actualizar.

DESCRiption (Obligatorio)

Especifica una descripción del grupo de nodos. Este parámetro es necesario. La longitud máxima de la descripción es de 255 caracteres. Si la descripción contiene blancos, encierre toda la descripción entre comillas.

Ejemplo: actualizar la descripción de un grupo de nodos

Actualizar el grupo de nodos, `group1`, con una nueva descripción.

```
update nodegroup group1 description="Recursos Humanos"
```

Mandatos relacionados



Tabla 1. Mandatos relacionados con UPDATE NODEGROUP

Mandato	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.




UPDATE PATH (cambiar una ruta)

Utilice este mandato para actualizar una definición de ruta.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de ruta.

- UPDATE PATH (Cambiar una ruta cuando el destino es una unidad)
- UPDATE PATH (Cambiar una ruta cuando el destino es una biblioteca)
-  Sistemas operativos AIX  Sistemas operativos Linux UPDATE PATH (Actualizar una ruta cuando el destino es una biblioteca ZOSMEDIA)

Si quiere obtener información detallada y actual sobre soporte de dispositivos, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE PATH

Mandato	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE PATH	Suprime una ruta de un origen a un destino.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

UPDATE PATH (Cambiar una ruta cuando el destino es una unidad)

Utilice esta sintaxis cuando actualice una definición de ruta a una unidad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType-----+--DATAMover--+-----+----->
      '-SERVer----'   '-AUTODetect-----+--No--+-'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY--nombre_biblioteca----->
>+-----+-----+-----+----->
      '-DEVICE-----nombre_dispositivo-'   '-ONLine-----+--Yes+-'
                                          '-No--'
>+-----+-----+-----+-----<<
|           .,-----, |
|           v           | |
'-DIRectory-----nombre_directorio+--'
```

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un servidor o un agente de almacenamiento.

AUTODetect

Especifica si se detectará, reportará y actualizará automáticamente el número de serie de una unidad o biblioteca en IBM Spectrum Protect. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad o a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente.

Yes

Especifica que el número de serie se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica a IBM Spectrum Protect.

Importante:

1. Si anteriormente no ha especificado un número de serie, AUTODETECT toma YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. AUTODETECT=YES en este mandato modifica el número de serie que se ha establecido en el mandato DEFINE DRIVE.
3. Si establece DESTTYPE=DRIVE y AUTODETECT=YES, el número de elemento de la unidad que se encuentra en la base de datos de IBM Spectrum Protect cambiará automáticamente para reflejar el mismo número de elemento que corresponde al número de serie de esa unidad. Esto se aplica a las unidades de una biblioteca SCSI. Para obtener más información acerca del número de elemento, consulte el mandato DEFINE DRIVE.
4. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

DESTType=DRive (Obligatorio)

Especifica que el destino es una unidad. Cuando el destino es una unidad, debe especificar un nombre de biblioteca. Este parámetro es necesario.

LIBRARY

Especifica el nombre de la biblioteca a la que se asigna la unidad. La biblioteca debe estar ya definida en el servidor. Si la ruta es de un transportador de datos NAS a una biblioteca, la biblioteca debe tener el LIBTYPE establecido en SCSI, 349x o ACSLS.

DEVICE

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.



 Sistemas operativos AIXEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos AIX/dev/rmt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM® System Storage Serie N: rst01


 Sistemas operativos LinuxEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	/dev/tmscsi/mt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	/dev/tmscsi/mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM System Storage Serie N: rst01



 Sistemas operativos WindowsEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 3 para obtener ejemplos.

Tabla 3. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos Windowsmt3
De servidor a unidad (unidad REMOVABLEFILE)	e:
De un agente de almacenamiento a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM System Storage Serie N: rst01

Importante:

- En las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el mandato SYSCONFIG. Utilice este mandato para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Por ejemplo, si la ruta desde un transportador de datos a una unidad está en línea, pero el transportador de datos o la unidad está fuera de línea, no puede utilizar la ruta.

DIRectory


Especifica la ubicación o ubicaciones de directorio de un agente de almacenamiento para el acceso a los archivos de una biblioteca FILE. El parámetro DIRECTORY también se utiliza para los dispositivos de tipo REMOVABLEFILE. Para los dispositivos REMOVABLEFILE, el parámetro DIRECTORY proporciona información para el servidor (no un agente de almacenamiento) junto con el parámetro DRIVE para describir acceso al dispositivo. Este parámetro es opcional.

En los agentes de almacenamiento, este parámetro sólo es válido cuando se cumplen *todas* las condiciones siguientes:

- El tipo de origen es SERVER (lo que significa que se ha definido como servidor un agente de almacenamiento en este servidor).
- El nombre de origen es el nombre del agente de almacenamiento y *no* del servidor.
- El destino es una unidad lógica que forma parte de una biblioteca FILE.
- Si se han especificado varios directorios para la clase de dispositivo que se asocia a la biblioteca FILE, debe especificarse, para cada unidad de la biblioteca FILE, el mismo número de directorios con el parámetro DIRectory del mandato DEFINE PATH. Los directorios de agente de almacenamiento no se validan en el servidor. Si se especifican directorios incorrectos, se puede producir una anomalía de tiempo de ejecución.

El nombre o nombres de directorio identifican las ubicaciones en las que el agente de almacenamiento lee y graba los archivos que representan volúmenes de almacenamiento para la clase de dispositivo FILE asociada a la biblioteca FILE. El valor predeterminado de DIRECTORY es el directorio del servidor en el momento en que se emite el mandato.

Utilice un convenio de denominación que le permita asociar el directorio a una unidad física determinada. Esto ayuda a garantizar que la configuración es válida para compartir la biblioteca FILE entre el servidor y el agente de almacenamiento. Si el agente de almacenamiento se encuentra en un sistema Windows, utilice un nombre del convenio de denominación universal (UNC). Cuando el agente de almacenamiento no disponga de permiso para acceder al almacenamiento remoto, el agente de almacenamiento sufrirá anomalías de montaje.

 Sistemas operativos Windows La cuenta asociada con el servicio del agente de almacenamiento debe ser una cuenta del grupo de administradores local o una cuenta del grupo de administradores del dominio. Si la cuenta está en el grupo de administradores local, el identificador de usuario y la contraseña deben corresponderse con los de la cuenta con autorización para acceder al almacenamiento, tal como fueron proporcionados por la máquina que administra los elementos compartidos remotos. Por ejemplo, si un servidor SAMBA proporciona acceso al almacenamiento remoto, el identificador de usuario y la contraseña de la configuración SAMBA deben coincidir con los del identificador de usuario y la contraseña del administrador local asociado al servicio del agente de almacenamiento.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path stal filel srctype=server desttype=drive
library=filel device=file directory=\\192.168.1.10\filedir\dir1
```


En el ejemplo anterior, el mandato DEFINE DEVCLASS establece el sistema de archivos compartidos en el directorio al que el servidor accede como D:\FILEDIR\DIR1. No obstante, el agente de almacenamiento, está utilizando un nombre UNC \\192.168.1.10\FILEDIR\DIR1. Esto implica que la máquina con la dirección TCP/IP 192.168.1.10 está compartiendo el mismo directorio, que utiliza FILEDIR como nombre compartido. Asimismo, el servicio del agente de almacenamiento tiene una cuenta que puede acceder a este almacenamiento. Puede acceder a éste porque está asociado a una cuenta local con el mismo identificador de usuario y contraseña que 192.168.1.10 o a una cuenta de dominio disponible tanto en el agente de almacenamiento como en 192.168.1.10. Si es adecuado para la instalación, puede sustituir 192.168.1.10 por un nombre simbólico como:

```
example.yourcompany.com
```

Importante:

- IBM Spectrum Protect no crea recursos compartidos, permisos ni monta el sistema de archivos destino. Debe realizar estas acciones antes de iniciar el agente de almacenamiento.


- Sólo puede modificar una lista de directorios sustituyendo la lista completa.
- Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para acceder a los volúmenes FILE, los agentes de almacenamiento sustituyen los nombres de la lista de directorios en la definición de clase de dispositivo por los nombres de la lista de directorios de la definición de ruta asociada. A continuación, se muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:  Sistemas operativos Windows

- o c:\server
- o d:\server
- o e:\server

 Sistemas operativos AIX  Sistemas operativos Linux


- o /opt/tivoli1
- o /opt/tivoli2
- o /opt/tivoli3

1. Utilice el siguiente mandato para configurar una biblioteca FILE denominada CLASSA con una unidad denominada CLASSA1 en SERVER1: 


```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```



2. Desea que el agente de almacenamiento STA1 pueda utilizar la biblioteca FILE, por lo tanto, define la siguiente ruta para el agente de almacenamiento STA1: 


```
define path server1 stal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

 Sistemas operativos Windows En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio c:\server por el nombre de directorio \\192.168.1.10\c\server para poder acceder a los volúmenes FILE que se encuentran en el directorio c:\server del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux



```
define path server1 stal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

 Sistemas operativos AIX  Sistemas operativos Linux En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio /opt/tivoli1 por el nombre de directorio /opt/ibm1/ para poder acceder a los volúmenes FILE que se encuentran en el directorio /opt/tivoli1 del servidor.

3.  Sistemas operativos Windows SERVER1 crea el volumen de archivo c:\server\file1.dsm. Si cambia más adelante el primer directorio de la clase de dispositivo con el mandato siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

SERVER1 todavía dispondrá de acceso al volumen de archivo c:\server\file1.dsm, pero el agente de almacenamiento STA1 no podrá acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociados a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE del directorio. Aunque todavía podrá accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

4.  Sistemas operativos AIX  Sistemas operativos Linux Si se crea el volumen de archivo /opt/tivoli1/file1.dsm en SERVER1, y se emite el siguiente mandato,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

SERVER1 todavía dispondrá de acceso al volumen de archivo /opt/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no podrá acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociados a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE del directorio. Aunque todavía podrá accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

Ejemplo: definir una ruta desde un servidor de archivos NAS de transportador de datos hasta una unidad de cintas

Actualizar una ruta desde un transportador de datos, que es un servidor de archivos NAS, hasta la unidad *TAPEDRV2* que el transportador de datos utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, el transportador de datos NAS es *NAS1*, la biblioteca es *NASLIB* y el nombre de dispositivo de la unidad es *rst01*.

```
update path nas1 tapedrv2 srctype=datamover desttype=drive library=naslib
device=rst01
```

UPDATE PATH (Cambiar una ruta cuando el destino es una biblioteca)

Utilice esta sintaxis cuando actualice una definición de ruta a una biblioteca.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType-----+-DATAMover-+---+-----+----->
      '-SERVer----'   '-AUTODetect-----+No--+-'
                          '-Yes-'
>--DESTType-----LIBRARY--+-+-----+----->
      +-DEVIce-----nombre_dispositivo---+
      '-EXTERNALManager-----nombre_ruta-'
>+-----+-----+-----+-----><
      '-ONLine-----+Yes-+-'
                          '-No--'
```

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

Importante: Para definir una ruta de un transportador de datos NAS a una biblioteca, la biblioteca debe tener LIBTYPE establecido en SCSI, 349X o ACSLS (Automated Cartridge System Library Software).

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un servidor o un agente de almacenamiento.

AUTODetect

Especifica si se detecta, notifica y actualiza automáticamente el número de serie de una unidad o biblioteca en IBM Spectrum Protect. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente.

Yes

Especifica que el número de serie se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica a IBM Spectrum Protect.

Importante:

1. Si anteriormente no ha especificado un número de serie, AUTODETECT toma YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.

2. AUTODETECT=YES en este mandato modifica el número de serie que se ha establecido en el mandato DEFINE DRIVE.
3. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

DESTType=LIBRARY (Obligatorio)

Especifica que el destino es una biblioteca. Este parámetro es necesario.

DEVICE

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.




 Sistemas operativos AIX El origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos AIX/dev/lb4  Sistemas operativos Linux /dev/tmscsi/lb4
De un transportador de datos NAS a una biblioteca	mc0


 Sistemas operativos Linux El origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	/dev/tmscsi/lb4
De un transportador de datos NAS a una biblioteca	mc0



 Sistemas operativos Windows El origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 3 para obtener ejemplos.

Tabla 3. Ejemplos de nombres de dispositivos


De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos Windows lb4.1
De un transportador de datos NAS a una biblioteca	mc0

Importante:

- En las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM® Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el mandato SYSCONFIG. Utilice este mandato para determinar el nombre de dispositivo para una biblioteca:

```
sysconfig -m
```

EXTERNALManager

Especifica la ubicación del gestor de bibliotecas externo donde IBM Spectrum Protect puede enviar peticiones de acceso a medio. Especifique el valor de este parámetro entre comillas simples. Por ejemplo, especifique:  Sistemas operativos AIX

```
/usr/lpp/GESedt-acsls/bin/elmdt
```

 Sistemas operativos Linux

```
/opt/GESedt-acsls/bin/elmdt
```

 Sistemas operativos Windows

```
C:\Archivos de programa\GES\EDT-ACSLs\bin\elmdt.exe
```

Este parámetro es necesario cuando el nombre de la biblioteca es una biblioteca externa.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Importante: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.

 Sistemas operativos AIX  Sistemas operativos Linux

UPDATE PATH (Actualizar una ruta cuando el destino es una biblioteca ZOSMEDIA)

Utilice esta sintaxis cuando actualice una ruta a una biblioteca ZOSMEDIA.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType----SERVer--DESTType----LIBRary----->
>--ZOSMEDIASERVER----server_name--+-----+-----><
                                   '-ONLine----+Yes-+-'
                                   '-No--'
```

Parámetros

nombre_origen (Obligatorio)

Especifica el nombre del origen de la ruta.

nombre_destino (Obligatorio)

Especifica el nombre del destino.

SRCType=SERVer (Obligatorio)

Especifica que el origen es el servidor de IBM Spectrum Protect o un agente de almacenamiento.

DESTType=LIBRary (Obligatorio)

Especifica que el destino es una biblioteca.

ZOSMEDIAServer (Obligatorio)

Especifica el nombre de servidor que representa un servidor de Tivoli Storage Manager for z/OS Media.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Importante: Si la ruta a una biblioteca está desactivada, el servidor no puede acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, la biblioteca no se inicializa durante la inicialización del servidor. Se debe actualizar la ruta a ONLINE=YES para acceder a la biblioteca.

UPDATE POLICYSET (Actualizar la descripción de un juego de políticas)

Utilice este mandato para cambiar la descripción de un juego de políticas. No puede cambiar la descripción del juego de políticas ACTIVE.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-UPDate Policyset--nombre_dominio--nombre_conjunto_políticas-->  
>--DEscription--===descripción-----><
```

Parámetros

nombre_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el juego de políticas.

nombre_juego_políticas (Necesario)

Especifica el juego de políticas que se actualiza. No puede cambiar el juego de políticas ACTIVE.

DEscription (Obligatorio)

Especifica el texto que describe el juego de políticas. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("").

Ejemplo: actualizar un juego de políticas

Actualizar un juego de políticas denominado VACATION para el dominio de políticas EMPLOYEE_RECORDS con la descripción "Schedule Planning Information".

```
update policyset employee_records vacation  
description="schedule planning information"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

UPDATE PROFILE (Actualizar una descripción de perfil)

Utilice este mandato en un gestor de configuración para actualizar una descripción de perfil.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate PROFIle--nombre_perfil--DEscription--===descripción--><
```

Parámetros

nombre_perfil (Obligatorio)

Especifica el perfil que se actualiza.

DESCription (Obligatorio)

Especifica una descripción del perfil. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para eliminar una descripción, especifique una serie nula ("").

Ejemplo: actualizar la descripción de un perfil

Actualizar la descripción del perfil DELTA.

```
update profile delta description="PAYROLL domain"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE PROFILE

Mandato	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.

UPDATE RECOVERYMEDIA (Actualizar medio de recuperación)

Utilice este mandato para actualizar la información sobre los medios de recuperación.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>>UPDate RECOVERYMedia--nombre_medio----->
>+-----+-----+-----+-----+----->
|           .,-----.|
|           v         ||
|'-VOLumenames-----nombre_volumen-+-'|
>+-----+-----+-----+-----+----->
|'-DESCription-----descripción-'
>+-----+-----+-----+-----+----->
|'-LOcation----ubicación-'  '-Type----+B0ot-+-'|
|                                     '-Other-'
>+-----+-----+-----+-----+----->
|'-PR0duct-----nombre_producto-'
>+-----+-----+-----+-----+-----<<
|'-PR0DUCTInfo-----información_producto-'
```

Parámetros

nombre_soporte (Obligatorio)

Especifica el nombre del medio de recuperación que se ha de actualizar.

VOLumentNames

Especifica los nombres de volúmenes que contienen datos recuperables (por ejemplo, copias de imágenes del sistema operativo). Si especifica TYPE=BOOT, debe especificar los nombres de los medios de arranque en el orden en que deben cargarse al efectuar la operación de recuperación. La lista de nombres de volúmenes puede tener hasta 255 caracteres. La lista debe estar delimitada por comillas si contiene algún carácter en blanco. Para eliminar todos los nombres de volúmenes, especifique una serie nula ("").

DESCRiption

Especifica la descripción del medio de recuperación. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

LOcation

Describe la ubicación del medio de recuperación. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para eliminar una descripción de ubicación, especifique una serie nula ("") como valor.

Type

Especifica el tipo de medio de recuperación. Este parámetro es opcional. Los valores posibles son:

BOot

Especifica que este es un medio de arranque. Debe especificar los nombres de los volúmenes si el tipo es BOOT.

OTHer

Especifica que éste no es un medio de arranque. Por ejemplo, un CD que contiene los manuales del sistema operativo.

PROduct

Especifica el nombre del producto que se ha grabado en este medio. Este parámetro es opcional. Puede utilizar hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un nombre de producto, especifique una serie nula ("") como valor.

PRODUCTInfo

Especifica la información acerca del producto que ha grabado en el medio que puede necesitar para restaurar la máquina. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para eliminar la información del producto definida anteriormente, especifique una serie nula ("") para el valor.

Ejemplo: actualizar la descripción de ubicación de los medios de recuperación

Actualizar la descripción de ubicación de los medios de recuperación DIST5RM por "Corporate Headquarters Data Vault."

```
update recoverymedia dist5rm
location="Corporate Headquarters Data Vault"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE RECOVERYMEDIA

Mandato	Descripción
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

UPDATE REPLRULE (Actualizar reglas de réplica)

Utilice este mandato para activar o desactivar una regla de réplica.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate REPLRule--nombre_regla----State---+--ENabled--+-+-----><
'-DISabled-'
```

Parámetros

nombre_regla (Obligatorio)

Especifica el nombre de la regla de réplica que se va a actualizar. Puede utilizar caracteres comodín para especificar una o varias reglas. Puede especificar una de las reglas siguientes:

- ALL_DATA
- ACTIVE_DATA
- ALL_DATA_HIGH_PRIORITY
- ACTIVE_DATA_HIGH_PRIORITY

State (Obligatorio)

Especifica si la réplica está permitida para la regla. Puede especificar uno de los siguientes valores:

ENabled

Especifica que los datos a los que se aplica la regla están preparados para replicarse.

DISabled

Especifica que la réplica no se realiza hasta que la activa.

Ejemplo: desactivar la réplica de datos de copia de seguridad

Desactive la réplica de los datos de copia de seguridad activos, de prioridad normal, para todos los espacios de archivos de todos los nodos de cliente que están configurados para la réplica:

```
update replrule active_data state=disabled
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE REPLRULE

Mandato	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

UPDATE SCHEDULE (Actualizar una planificación)

Utilice este mandato para actualizar una planificación de cliente o de mandato de administración.

El mandato UPDATE SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones cliente o a mandatos de administración. En estos dos formatos, puede seleccionar las planificaciones de estilo clásico o mejorado. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con UPDATE SCHEDULE

Mandato	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un mandato de administración.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un mandato planificado.
SET MAXSCHEDESESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

- UPDATE SCHEDULE (Actualizar una planificación de cliente)
Utilice el mandato UPDATE SCHEDULE para actualizar parámetros seleccionados de una planificación de cliente.
- UPDATE SCHEDULE (Actualizar una planificación de administración)
Utilice este mandato para actualizar los parámetros seleccionados de una planificación de mandatos de administración.

UPDATE SCHEDULE (Actualizar una planificación de cliente)

Utilice el mandato UPDATE SCHEDULE para actualizar parámetros seleccionados de una planificación de cliente.

Este mandato no cambia las asociaciones de cliente que se han realizado en esta planificación. Todos los clientes asociados a la planificación original procesan la planificación modificada.

No todos los clientes pueden ejecutar todas las operaciones planificadas, aunque pueda definir la planificación en el servidor y asociar ésta al cliente. Por ejemplo, un cliente Macintosh no puede ejecutar una planificación cuando la acción sea restaurar o recuperar archivos o ejecutar un script ejecutable. En los diferentes sistemas operativos cliente, un script ejecutable, también se conoce como un archivo de mandatos, un archivo por lotes o un script.

Clase de privilegio

Para definir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado al dominio de políticas al que pertenece la planificación.

Sintaxis correspondiente a una planificación de cliente clásica

```

(1)
>>-UPDate SChedule----->
>--nombre_dominio--nombre_planificación--+-----+>
|                                     |'-Type-----Client-'|
>+-----+>
|'-DEScRiption-----descripción-'|
>+-----+>
|'-ACTion-----+Incremental-----+-'|
|   +-Selectiva-----+|
|   +-Archive--+-----+|
|   |           |         |'-SUBACTion-----+-----+-'|
|   |           |         |'-FASTBack-'|
|   +-Backup--+-----+|
|   |           |         |'-SUBACTion-----+-----+-'|
|   |           |         |'+FASTBack----+|
|   |           |         |'+SYSTEMState+|
|   |           |         |'-VM-----'|

```



```

+-REStore-----+
+-REtrieve-----+
+-IMAGEBACKup-----+
+-IMAGEREStore-----+
+-Command-----+
+-Macro-----+
'-Deploy-----'

>+-----+
'-OPTions---serie_opción-' '-OBJects---serie_objeto-'

>+-----+
'-PRIority---número-' '-STARTDate---fecha-'

>+-----+
'-STARTTime---hora-' '-DURation ---número-'

>+-----+
'-DURUnits---Minutes-----' '-MAXRUNTime---número-'
  +-Hours-----+
  +-Days-----+
  '-INDefinite-'

>+-----+
'-SCHEDStyle---Classic-' '-PERiod---número-'

>+-----+
'-PERUnits---Hours-----'
  +-Days-----+
  +-Weeks---+
  +-Months---+
  +-Years---+
  '-Onetime-'

>+-----+
'-DAYofweek---ANY-----+'
  +-WEEKDay---+
  +-WEEKEnd---+
  +-SUNDay---+
  +-Monday---+
  +-TUESday---+
  +-WednesDay+
  +-THURsday---+
  +-FRIday---+
  '-SATurday--'

>+-----+<
'-EXPiration---Never---+'
  '-date--'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.

Sintaxis correspondiente a una planificación de cliente mejorada

```

(1)
>>-UPDate SCHEDULE-----+
>---nombre_dominio---nombre_planificación---+-----+
                                     '-Type---Client-'

>+-----+
'-DESCRiption---descripción-'

>+-----+
'-ACTion---Incremental-----+'
  +-Selectiva-----+
  +-Archive---+-----+
  |         '-SUBACTion---+-----+' |
  |                                     '-FASTBack-' |
  +-Backup---+-----+
  |         '-SUBACTion---+-----+' |
  |                                     +-FASTBack---+ |

```

```

      |                               +-SYSTEMState+ |
      |                               +-VApp-----+ |
      |                               '-VM-----'  |
+-REStore-----+
+-REtrieve-----+
+-IMAGEBACKup-----+
+-IMAGERESTore-----+
+-Command-----+
'-Macro-----'

>+-----+-----+-----+-----+----->
  '-OPTions----serie_opción-' '-OBJects----serie_objeto-'

>+-----+-----+-----+-----+----->
  '-PRIority----número-' '-STARTDate----fecha-'

>+-----+-----+-----+-----+----->
  '-STARTTime----hora-' '-DURation ----número-'

>+-----+-----+-----+-----+----->
  '-DURUnits----+Minutes--+' '-MAXRUNtime----número-'
                        +-Hours---+
                        '-Days----'

>+-----+-----+-----+-----+----->
  '-SCHEDStyle----Enhanced-' '-MONth----+ANY-----+'
                               +-January---+
                               +-February--+
                               +-MARch-----+
                               +-APRil-----+
                               +-May-----+
                               +-JUNE-----+
                               +-JULy-----+
                               +-August----+
                               +-September+
                               +-October---+
                               +-November--+
                               '-December--'

>+-----+-----+-----+-----+----->
  '-DAYOFMonth----+ANY++' '-WEEKofmonth----+ANY----+'
                        '-Day-'                +-First--+
                                                    +-Second+
                                                    +-Third--+
                                                    +-FOurth+
                                                    '-Last---'

>+-----+-----+-----+-----+----->
  '-DAYofweek----+ANY-----+'
                        +-WEEKDay---+
                        +-WEEKEnd---+
                        +-SUnDay----+
                        +-Monday----+
                        +-TUESday---+
                        +-WednesDay--+
                        +-THURsday--+
                        +-FRIday----+
                        '-SATurday--'

>+-----+-----+-----+-----+-----><
  '-EXPIration----+Never++'
                        '-date--'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de actualizar.

Type=Client

Especifica que se actualiza una planificación de cliente. Este parámetro es opcional. El valor predeterminado es CLIENT.

DESCRiption

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula (""") para este valor.

ACTiion

Especifica la acción que se produce cuando se procesa esta planificación. Los valores posibles son:

Incremental

Especifica que la planificación hace copia de seguridad de todos los archivos que son nuevos o que se han modificado desde la última copia de seguridad incremental. La copia de seguridad incremental también hace copia de seguridad de todos los archivos para el que se hayan podido caducar todas las copias de seguridad existentes.

Selective

Especifica que la planificación sólo hace copia de seguridad de los archivos especificados con el parámetro OBJECTS.

Archive

Especifica que la planificación hace copia archivada de los archivos especificados con el parámetro OBJECTS.

Backup

Especifica que la planificación realiza una copia de seguridad de los archivos especificados con el parámetro OBJECTS.

REStore

Especifica que la planificación restaura los archivos especificados con el parámetro OBJECTS.

Quando especifique ACTION=RESTORE para una operación planificada y se define la opción REPLACE como PROMPT, no se efectúa ninguna petición. Si establece la opción en PROMPT, se ignoran los archivos.

Si se especifica una segunda especificación de archivo, ésta actúa como destino de la restauración. Si necesita restaurar varios grupos de archivos, planifique una restauración para cada especificación de archivo que necesita restaurar.

RETrieve

Indica que la planificación recupera los archivos especificados con el parámetro OBJECTS.

Recuerde: Un segundo archivo especificado actúa como el destino de recuperación. Si necesita recuperar varios grupos de archivos, cree una planificación distinta para cada grupo de archivos.

IMAGEBACKup

Especifica que la planificación hace copia de seguridad de los volúmenes lógicos especificados con el parámetro OBJECTS.

IMAGERESStore

Especifica que la planificación restaura los volúmenes lógicos especificados con el parámetro OBJECTS.

Mandato

Indica que la planificación procesa un mandato de un sistema operativo de cliente o un script, especificado con el parámetro OBJECTS.

Macro

Especifica que un cliente procesa una macro cuyo nombre de archivo se especifica con el parámetro OBJECTS.

SUBACTiion

Puede especificar uno de los siguientes valores:

""

Quando una serie vacía (dos dobles comillas) se especifica con ACTION=BACKUP, la copia de seguridad es incremental.

FASTBACk

Especifica que una operación de cliente FastBack identificada por el parámetro ACTION se va a planificar para procesar. El parámetro ACTION debe ser ARCHIVE o BACKUP.

SYSTEMState

Especifica que se ha programado una copia de seguridad del estado del sistema.

VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

VM

Especifica que se ha programado una copia de seguridad VMware del cliente.

Deploy

Especifica si se actualizarán las estaciones de trabajo del cliente con paquetes de despliegue especificados con el parámetro OBJECTS. El parámetro OBJECTS debe contener dos especificaciones: los archivos del paquete que se deben recuperar y de dónde recuperarlos. Asegúrese de que los objetos están en orden *ubicación_archivos*. Por ejemplo:

```
define schedule standard deploy_1 action=DEPLOY objects=  
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\  
..\IBM_ANR_WIN\"
```

Los valores de las siguientes opciones estarán restringidos si se especifica ACTION=DEPLOY:

PERUNITS

Especifique PERUNITS=ONETIME. Si especifica PERUNITS=PERIOD, el parámetro se omitirá.

DURUNITS

Especifique MINUTES, HOURS o DAYS para el parámetro DURUNITS. No especifique INDEFINITE.

SCHEDSTYLE

Especifique el estilo predeterminado, CLASSIC.


El mandato SCHEDULE falla si los parámetros no coinciden con los valores de parámetro necesarios, como V.R.M.F.

OPTions

Especifica las opciones que se especifican en el mandato planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el mandato planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de mandatos. Todas las opciones que se describen como válidas solamente en la línea de mandatos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el mandato planificado:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el mandato DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el mandato planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:
 - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Para especificar `domain all-local -c: -d:`, escriba:
 - `options='-domain="all-local -c: -d:"'`

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

OBJects

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando ACTION=INCREMENTAL. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un mandato o una macro, el objeto será el nombre del mandato o macro que debe ejecutarse.

Si especifica ACTION=INCREMENTAL sin especificar ningún valor para este parámetro, el mandato planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número excesivo de argumentos de línea de mandatos
```

Si especifica ACTION=ARCHIVE, INCREMENTAL o SELECTIVE para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.

Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofes. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofes. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar C:\ARCHIVO 2, D:\ARCHIVOS GIF y E:\ARCHIVO DE PRUEBA, escriba:
 - OBJECTS=' "C:\ARCHIVO 2" "D:\ARCHIVOS GIF" "E:\ARCHIVO DE PRUEBA" '
- Para especificar D:\ARCHIVO DE PRUEBA, escriba:
 - OBJECTS=' "D:\ARCHIVO DE PRUEBA" '
- Para especificar D:\PRUEBA,ARCHIVO:
 - OBJECTS=' "'D:\PRUEBA,ARCHIVO"' '

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar /home/archivo 2, /home/archivos gif y /home/archivo de prueba, escriba:
 - OBJECTS=' "/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba" '
- Para especificar /home/archivo de prueba, escriba:
 - OBJECTS=' "/home/archivo de prueba" '

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de mandatos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.

Valor	Descripción	Ejemplo
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

Consejo: Defina las planificaciones con duraciones de más de 10 minutos. Con ello, el planificador de IBM Spectrum Protect dispondrá de tiempo suficiente para procesar la planificación y avisar al cliente.

DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

Minutes

Especifica que la duración del margen se define en minutos.

Hours

Especifica que la duración del margen se define en horas.

Days

Especifica que la duración del margen se define en días.

INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejo: El tiempo máximo de ejecución se calcula desde el principio de la ventana de inicio y no desde la hora en que se inician las sesiones en la ventana de inicio.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y no se emite ningún mensaje de aviso. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de una operación planificada son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todas las sesiones de cliente para esta operación deben finalizar a la 1:00 del mediodía. Si se siguen ejecutando una o varias sesiones después de la 1:00 del mediodía, el servidor emite un mensaje de aviso.

Consejo: También puede especificar un valor para *Alerta de tiempo de ejecución* de 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se puede ejecutar una planificación, o los días en los que se puede ejecutar. El estilo puede ser clásica o mejorada. Este parámetro debe especificarse al cambiar una planificación de clásica a mejorada o de mejorada a clásica. En caso contrario, se utiliza el valor para la planificación existente.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH. Si el estilo de planificación anterior fuese el mejorado, se restablecen los parámetros MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. DAYOFWEEK, PERIOD y PERUNITS se establecen como valores predeterminados a menos que estén especificados con el mandato de actualización.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS. Si el estilo de planificación anterior fuese el clásico, se restablecen los parámetros DAYOFWEEK, PERIOD y PERUNITS. MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK se establecen como valores predeterminados a menos que estén especificados con el mandato de actualización.

PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

Days

Especifica que el período entre márgenes de puesta en marcha es en días.

Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUESday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

Saturday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada mes del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es el -1, el penúltimo es el -2. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecuta una vez ese día.

El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

Si una planificación existente especifica un valor distinto a ANY para DAYOFWEEK y WEEKOFMONTH y se actualiza DAYOFMONTH, DAYOFWEEK y WEEKOFMONTH se restablecen a ANY.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecuta una vez durante esa semana.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

EXpiration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

Ejemplo: actualización de la prioridad de una planificación

Actualizar la planificación MONTHLY_BACKUP que pertenece al dominio de políticas STANDARD estableciendo su valor de prioridad en 1.

```
update schedule standard monthly_backup priority=1
```

Ejemplo: actualización de la fecha de caducidad de una planificación

Actualizar la planificación WEEKLY_BACKUP que pertenece al dominio de políticas EMPLOYEE_RECORDS de modo que caduque el 29 de Marzo de 1999 (03/29/1999).

```
update schedule employee_records weekly_backup expiration=03/29/1999
```

Ejemplo: actualizar una planificación para que el archivado se realice el último viernes del mes

Actualizar una planificación de las copias archivadas trimestralmente el último viernes del mes para archivarlas el último día de los meses especificados.

```
update schedule employee_records quarterly_archive dayofmonth=-1
```

WEEKOFMONTH y DAYOFWEEK se restablecen a ANY.

UPDATE SCHEDULE (Actualizar una planificación de administración)

Utilice este mandato para actualizar los parámetros seleccionados de una planificación de mandatos de administración.

No puede planificar mandatos MACRO ni QUERY ACTLOG.

Una planificación de administración gestionada que se actualiza por medio de un gestor de configuración se establece en un estado inactivo en los servidores gestionados durante el proceso de renovación de configuración. Permanece en un estado inactivo hasta que se actualiza a un estado activo en esos servidores.

Clase de privilegio

Para actualizar una planificación de administración, debe tener privilegio de sistema.

Sintaxis

Planificación de administración clásica

```
(1)
>>-UPDate SCHEDULE-----nombre_planificación----->
>--+-----+--+-----+----->
  '-Type---Administrative-' '-CMD---mandato-'
>--+-----+--+-----+----->
  '-ACTIVE---+Yes-+' '-DESCRIPTION---descripción-'
    '-No--'
>--+-----+--+-----+----->
  '-PRIORITY---número-' '-STARTDate---fecha-'
>--+-----+--+-----+----->
  '-STARTTime---hora-' '-DURATION ---número-'
>--+-----+--+-----+----->
  '-DURUnits---+Minutes---+' '-MAXRUNTime---número-'
    '+Hours-----+
    '+Days-----+
    '-INDefinite-'
>--+-----+--+-----+----->
  '-SCHEDStyle---Classic-' '-PERiod---número-'
>--+-----+--+-----+----->
  '-PERUnits---+Hours---+'
    '+Days----+
    '+Weeks---+
    '+Months---+
    '+Years---+
    '-Onetime-'
>--+-----+--+-----+----->
  '-DAYofweek---+ANY-----+'
    '+WEEKDay---+
    '+WEEKEnd---+
    '+SUNday----+
    '+MONday----+
    '+TUESday---+
    '+WEDnesday--+
    '+THURsday--+
    '+FRIDay----+
    '-SATurday--'
>--+-----+--+-----+-----><
  '-EXPIration---+Never---+'
    '-date--'
```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.

Sintaxis

Planificación de administración mejorada

```
(1)
>>-UPDate SCHEDULE-----nombre_planificación----->
>--+-----+--+-----+----->
  '-Type-----Administrative-' '-CMD-----mandato-'
>--+-----+--+-----+----->
  '-ACTIVE-----+Yes+-' '-DESCRiption-----descripción-'
    '-No--'
>--+-----+--+-----+----->
  '-PRIority-----número-' '-STARTDate-----fecha-'
>--+-----+--+-----+----->
  '-STARTTime-----hora-' '-DURation -----número-'
>--+-----+--+-----+----->
  '-DURUnits-----+Minutes+-' '-MAXRUNtime-----número-'
    '+Hours---'
    '-Days----'
>--+-----+--+-----+----->
  '-SCHEDStyle-----Enhanced-' '-MONth-----+ANY-----+'
                                     +-January---+
                                     +-February---+
                                     +-MARch-----+
                                     +-APRil-----+
                                     +-May-----+
                                     +-JUNE-----+
                                     +-JULy-----+
                                     +-AUGust-----+
                                     +-September--+
                                     +-October---+
                                     +-November--+
                                     '-December--'
>--+-----+--+-----+----->
  '-DAYOFMonth-----+ANY+-' '-WEEKofmonth-----+ANY-----+'
    '-Day-'
                                     +-First--+
                                     +-Second+
                                     +-Third--+
                                     +-FOurth+
                                     '-Last---'
>--+-----+--+-----+----->
  '-DAYofweek-----+ANY-----+'
    +-WEEKDay---+
    +-WEEKEnd---+
    +-SUnday----+
    +-Monday----+
    +-TUESday---+
    +-WednesDay--+
    +-THURsday--+
    +-FRIday----+
    '-SATurday--'
>--+-----+--+-----+-----><
  '-EXPIration-----+Never+-'
    '-date--'
```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.

Parámetros

nombre_planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de actualizar.

Type=Administrative (Necesario)

Especifica que se actualiza una planificación de mandatos de administración.

CMD

Especifica el mandato de administración que se planificará para procesarlo. Este parámetro es opcional. El mandato que especifique puede contener hasta 512 caracteres. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco.

No puede especificar caracteres de redirección con este parámetro.

ACTIVE

Especifica si el mandato de administración puede seleccionarse para procesarlo. Este parámetro es opcional. Las planificaciones de mandatos de administración no se procesan si no se establecen en el estado activo. Los valores posibles son:

YES

Especifica que el mandato de administración puede seleccionarse para procesarlo.

NO

Especifica que el mandato de administración no puede seleccionarse para procesarlo.

DEscription

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("") para este valor.

PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este mandato a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o - HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

Minutes

Especifica que la duración del margen se define en minutos.

Hours

Especifica que la duración del margen se define en horas.

Days

Especifica que la duración del margen se define en días.

INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales se deben completar los procesos del servidor que se han iniciado mediante los mandatos planificados. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejos:

- Es posible que los procesos no finalicen inmediatamente después de que los haya cancelado el planificador central. Finalizan cuando registran la notificación de cancelación del planificador central.
- El tiempo de ejecución máximo se calcula comenzando desde el momento en que se inicia el servidor. Si el mandato de planificación inicia más de un proceso, se calcula tiempo máximo de ejecución de cada proceso a partir del inicio del proceso.
- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.

- Este parámetro no se aplica si el mandato planificado no inicia un proceso de servidor.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

Este parámetro es opcional. Puede especificar un número en el rango de 0-1440. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y el planificador central no cancela los procesos. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de un mandato planificado son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todos los procesos de servidor aplicables iniciados por el mandato se deben finalizar a la 1:00 del mediodía. Si uno o varios procesos aplicaciones continúan ejecutándose pasadas la 1:00 del mediodía, el planificador central cancela los procesos.

Consejo: También puede especificar como *hora de finalización* la 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se debe ejecutar una planificación, o los días en los que se debe ejecutar. El estilo puede ser clásica o mejorada. Este parámetro debe especificarse al cambiar una planificación de clásica a mejorada o de mejorada a clásica. En caso contrario, se utiliza el valor para la planificación existente.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH. Si el estilo de planificación anterior fuese el mejorado, se restablecerían los parámetros MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. DAYOFWEEK, PERIOD y PERUNITS se establecerán como valores predeterminados a menos que estén especificados con el mandato de actualización.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS. Si el estilo de planificación anterior fuese el clásico, se restablecerían los parámetros DAYOFWEEK, PERIOD y PERUNITS. MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK se establecerán como valores predeterminados a menos que estén especificados con el mandato de actualización.

PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

Days

Especifica que el período entre márgenes de puesta en marcha es en días.

Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir

de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUESday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

SATurday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY. Esto

significa que la planificación se ejecutará todos los meses del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Sólo se puede especificar este parámetro con planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es -1, el penúltimo es -2, etc. Puede especificar varios valores separados mediante comas, sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecutará una vez ese día.

El valor predeterminado es ANY. Esto significa que la planificación se ejecutará cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Sólo se puede especificar este parámetro con planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecutará una vez durante esa semana.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

EXPIration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

Ejemplo: actualizar una planificación de copia de seguridad para que ésta se realice cada tres días

Actualizar una planificación de administración existente denominada BACKUP_BACKUPPOOL, de modo que, a partir de hoy, se realice una copia de seguridad de la agrupación de almacenamiento primaria BACKUPPOOL en la agrupación de almacenamiento de copia COPYSTG cada tres días a las 22:00 horas.

```
update schedule backup_backuppool type=administrative cmd="backup
stgpool backuppool copystg" active=yes starttime=22:00 period=3
```

Ejemplo: actualizar una planificación de copia de seguridad para que se realice el primer y el tercer viernes de cada mes

Actualizar una planificación denominada BACKUP_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. La planificación existente se ejecuta el primer y el décimo día de cada mes. Actualícelo para ejecutarse el primer y el tercer viernes de cada mes.

```
update schedule backup_archivepool
dayofweek=friday
weekofmonth=first,third
```

DAYOFMONTH se restablecerá a ANY.

UPDATE SCRATCHPADENTRY (Actualizar una entrada de registro)

Utilice este mandato para actualizar datos en una línea en el registro.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate SCRATCHPAdentry--major_category--minor_category----->
>--subject--Line ---número--Data----datos-----><
```

Parámetros

major_category (obligatorio)
Especifica la categoría principal en la que los datos se van a actualizar. Este parámetro distingue entre mayúsculas y minúsculas.

minor_category (obligatorio)
Especifica la categoría secundaria en la que se actualizarán los datos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)
Especifica el asunto bajo el que se actualizarán los datos. Este parámetro distingue entre mayúsculas y minúsculas.

Line (obligatorio)
Especifica el número de la línea en la que se actualizarán los datos.

Data (obligatorio)
Especifica los datos nuevos que se almacenarán en la línea. Se suprimen los datos anteriores. Puede entrar un máximo de 1000 caracteres. Ponga los datos entre comillas si los datos contienen uno o más espacios en blanco. Los datos distinguen entre mayúsculas y minúsculas.

Ejemplo: Actualizar una entrada de registro

Actualice los detalles de contacto de vacaciones de un administrador, Jane, en una base de datos que almacena información sobre la ubicación de todos los administradores:

```
update scratchpAdentry admin_info location jane line=2 data=
"Fuera de la oficina hasta el 18 de Nov."
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE SCRATCHPADENTRY

Mandato	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.

UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)

Utilice este mandato para cambiar una línea de mandatos existente o para agregar una nueva línea de mandatos a un script de IBM Spectrum Protect.

Restricción: No puede redirigir la salida de un mandato desde un script de IBM Spectrum Protect. En su lugar, ejecute el script, y luego especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

Clase de privilegio

Para emitir este mandato, el administrador debe haber definido el script con anterioridad o debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate SCRipt--nombre_script----->
>--+-----+----->
  '-línea_mandatos--+-----+'
    '-Line ---número-'
>--+-----+-----><
```

'-DESCRiption-----descripci3n-'

Parámetros

nombre_script (Obligatorio)

Especifica el nombre del script que se va a actualizar.

línea_mandatos

Especifica el mandato nuevo o actualizado que se procesará en un script. Al emitir este mandato, debe actualizar un mandato, una descripción o ambos.

El mandato puede contener variables de sustitución y se puede continuar en varias líneas si especifica un carácter de continuación (-) como último carácter del mandato. Puede especificar hasta 1200 caracteres para el mandato. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco. Si especifica este parámetro, opcionalmente puede especificar el parámetro siguiente.

Tiene las opciones de ejecutar los mandatos en serie, en paralelo o en serie y en paralelo, especificando los mandatos de script SERIAL o PARALLEL para este parámetro. Puede ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente. Los mandatos se ejecutarán en serie hasta que se encuentre un mandato en paralelo.

Pueden utilizarse sentencias de flujo lógico condicional. Estas sentencias incluyen IF, EXIT y GOTO.

Line

Especifica el número de línea del mandato. Si no especifica un número de línea, la línea de mandatos se agregará al final de la serie de líneas de mandatos existente. Se asignará a la línea de mandatos agregada un número de línea cinco unidades mayor que el último número de línea de mandatos de la secuencia. Por ejemplo, si la última línea del script es 015, a la línea de mandatos agregada se asigna el número 020.

Si especifica un número de línea, el mandato sustituirá una línea existente (si el número es el mismo que el de una línea existente). O insertará la línea especificada (si el número de línea no se corresponde con un número de línea existente de la secuencia de línea de mandatos).

DESCRiption

Especifica la descripción del script. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: agregar un mandato al final de un script

Imaginemos que ha definido el siguiente script de tres líneas, denominado QSAMPLE, y que desea agregar el mandato QUERY SESSION al final del script.

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY PROCESS
```

```
update script qsample "query session"
```

Después de haberse procesado el mandato, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION
```

Ejemplo: actualizar una línea específica de un script

Mediante la utilización del script del ejemplo anterior, cambiar la línea 010 para que procese el mandato QUERY STGPOOL en lugar del mandato QUERY PROCESS:

```
update script qsample "query stgpool" line=010
```

Después de haberse procesado el mandato, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY STGPOOL
015 QUERY SESSION
```

Ejemplo: insertar un mandato en la parte central de un script

Mediante la utilización del script del ejemplo anterior, inserte una nueva línea de mandatos (QUERY NODE OPEN) después de la línea de mandatos QUERY STATUS del script QSAMPLE:

```
update script qsample "query node"  
line=007
```

Después de haberse procesado el mandato, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */  
005 QUERY STATUS  
007 QUERY NODE  
010 QUERY STGPOOL  
015 QUERY SESSION
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE SCRIPT

Mandato	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.

Tareas relacionadas:

Ejecución de mandatos en paralelo o en serie
Inclusión de sentencias de flujo lógico en un script
Realización de tareas simultáneamente en varios servidores
Definición de un script del servidor

Referencia relacionada:

Códigos de retorno de los scripts para IBM Spectrum Protect

UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)

Utilice este mandato para actualizar la definición de un servidor.



Restricción: Si el servidor es un servidor de origen para una operación de volumen virtual, cambiar cualquiera de estos valores puede afectar a la capacidad del servidor de origen de acceder y gestionar los datos que están almacenados en el servidor de destino correspondiente. Cambiar el nombre del servidor utilizando el mandato SET SERVERNAME podría tener implicaciones adicionales, que varían en función del sistema operativo. Los siguientes son los valores posibles:

- Puede que las contraseñas dejen de ser válidas.
- Puede que la información de dispositivos se vea afectada.
- La información de registro sobre sistemas operativos Windows puede cambiar

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis de:

- **Configuración de Enterprise**
- **Anotación de eventos Enterprise**
- **Direccionamiento de mandatos**
- **Agente de almacenamiento**
- **Servidores de origen y destino de réplica de nodos**
-  Sistemas operativos AIX  Sistemas operativos Linux **servidor de medios de z/OS**

```


>>-UPDate--SERver--nombre_servidor----->
>+-----+-----+-----+-----+----->
  '-SERVERPAssword---contraseña-'
>+-----+-----+-----+-----+----->
  '-HLAddress---ip_address-' '-LLAddress---puerto_tcp-'
>+-----+-----+-----+-----+----->
  '-COMMmethod---TCPIP-' '-URL---url-'
>+-----+-----+-----+-----+----->
  '-ALLOWReplace---+Yes-+'
                               '-No--'
>+-----+-----+-----+-----+----->
  '-DEScRiption---descripción-' '-FORCESync---+Yes-+'
                                               '-No--'
>+-----+-----+-----+-----+----->
  | (1) |
  '-----VALIdateprotocol---+No---+'
                               '-All-'
>+-----+-----+-----+-----+----->
  '-SSL---+No---+'
                '-Yes-'

.-SESSIONSECurity---TRANSitional-----
>+-----+-----+-----+-----+----->
  '-SESSIONSECurity---+STRict-----+'
                               '-TRANSitional-'

.-TRANSFERMethod---Tcpi-----
>+-----+-----+-----+-----+----->
  '-TRANSFERMethod---+Tcpi---+'
                               | (2) |
                               '-Fasp-----'

```

Notas:

1. El parámetro VALIDATEPROTOCOL está en desuso y sólo se aplica a las definiciones del agente de almacenamiento.
2.  Sistemas operativos Linux El parámetro TRANSFERMETHOD solo está disponible en sistemas operativos Linux x86_64 .

Sintaxis correspondiente a volúmenes virtuales

```

>>-UPDate--SERver--nombre_servidor----->
>+-----+-----+-----+-----+----->
  '-PASSword---contraseña-' '-HLAddress---ip_address-'
>+-----+-----+-----+-----+----->
  '-LLAddress---puerto_tcp-' '-COMMmethod---TCPIP-'
>+-----+-----+-----+-----+----->
  '-URL---url-' '-DELgraceperiod---días-'
>+-----+-----+-----+-----+----->
  '-NODEName---nombre_nodo-' '-SSL---Yes-'

.-SESSIONSECurity---TRANSitional-----
>+-----+-----+-----+-----+----->
  '-SESSIONSECurity---+STRict-----+'
                               '-TRANSitional-'

.-FORCESync---+Yes-+' '-DEScRiption---descripción-'
                               '-No--'

```

Parámetros

nombre_servidor (Obligatorio)

Especifica el nombre del servidor que se va a actualizar. Este parámetro es necesario.

PAssword

Especifica la contraseña que se utiliza para iniciar la sesión en el servidor de destino para los volúmenes virtuales. Este parámetro es opcional.

SERVERPAssword

Especifica la contraseña del servidor, que se utiliza para las funciones de configuración de enterprise, direccionamiento de mandatos y anotación de eventos de servidor a servidor. Esta contraseña debe coincidir con la contraseña del servidor que se ha establecido con el mandato SET SERVERPASSWORD. Este parámetro es opcional.

HLAddress

Especifica la dirección IP (con formato de coma decimal) del servidor. Este parámetro es opcional.

LLAddress

Especifica la dirección de bajo nivel del servidor. Esta dirección suele coincidir con la dirección de la opción de servidor TCPPOINT del servidor destino. Cuando SSL=YES, el puerto ya debe estar designado para comunicaciones SSL en el servidor de destino.

COMMmethod

Especifica el método de comunicación que se utiliza para conectar con el servidor. Este parámetro es opcional.

URL

Especifica la dirección de URL que se utiliza para acceder a este servidor desde Centro de administración. El parámetro es opcional.

DELgraceperiod

Especifica un número de días en que el objeto permanece en el servidor de destino después de haber sido marcado para suprimirlo. Puede especificar un valor de 0 a 9999. El valor predeterminado es 5. Este parámetro es opcional.

NODENAME

Especifica un nombre de nodo que ha de utilizar el servidor para conectarse con el servidor destino. Este parámetro es opcional.

DESCRIPTION

Especifica la descripción del servidor. Este parámetro es opcional. La descripción puede tener hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

FORCESync

Especifica si se restablece la clave de verificación del servidor en la siguiente conexión del servidor origen con el servidor destino. Una clave de verificación válida permite que un servidor origen pueda colocar nuevos objetos en el servidor destino, gestionar el valor del período de gracia para la supresión y actualizar la contraseña, si se conoce la contraseña actual y coincide la clave de verificación. El parámetro es opcional. Puede especificar uno de los siguientes valores:

Yes

Especifica que se enviará una nueva clave de verificación al servidor destino y que éste la aceptará si se recibe una contraseña válida.

No

Especifica que no se enviará una nueva clave de verificación al servidor destino.

VALIDATEprotocol (en desuso)

Especifica si una comprobación de redundancia cíclica valida los datos enviados entre el agente de almacenamiento y el servidor de IBM Spectrum Protect. El parámetro es opcional. El valor predeterminado es NO.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2 y Tivoli Storage Manager Versión 7.1.8, la validación que está habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

ALLOWReplace

Especifica si una definición de servidor que ha definido un servidor gestionado puede sustituirse por una definición del gestor de configuración. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Yes

Especifica que una definición de servidor puede sustituirse por una definición del gestor de configuración.

No

Especifica que una definición de servidor no puede sustituirse por la definición del gestor de configuración.

SSL

Especifica la modalidad de comunicación del servidor.

Importante: A partir de IBM Spectrum Protect V8.1.2 y Tivoli Storage Manager V7.1.8, se utiliza SSL para cifrar ciertas comunicaciones con el servidor especificado, incluso si se especifica NO.

Las siguientes condiciones y consideraciones se aplican cuando especifica el parámetro SSL:

- Antes de iniciar los servidores, los certificados autofirmados de los servidores asociados deben estar en el archivo de base de datos de claves (cert.kdb) de cada uno de los servidores.
- Puede definir varios nombres de servidor con distintos parámetros en el mismo servidor de destino.

Puede especificar uno de los siguientes valores:

No

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, excepto si el servidor envía o recibe datos de objeto. Los datos de objeto se envían y se reciben mediante TCP/IP. Si elige no cifrar los objetos de datos, el rendimiento del servidor será similar a la comunicación mediante una sesión TCP/IP y la sesión es segura.

Yes

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, incluso si el servidor envía o recibe datos de objeto.

SESSIONSECurity

Especifica si el servidor que está definiendo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el servidor que se define. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor especificado y un servidor IBM Spectrum Protect.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el servidor especificado pueda autenticarse en el servidor IBM Spectrum Protect:

- Tanto el servidor que se define como el servidor IBM Spectrum Protect deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el servidor que está definiendo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre él mismo y el servidor IBM Spectrum Protect.


Los servidores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en IBM Spectrum Protect.

TRANSitional

Especifica que se aplican los valores de seguridad existentes para el servidor. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el servidor no cumplen nunca los requisitos para el valor STRICT, el servidor continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un servidor cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el servidor ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un servidor que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, el direccionamiento de mandatos o la exportación entre servidores, cuando un nodo o un administrador se autentica en el servidor IBM Spectrum Protect como nodo o administrador de otro servidor.

Sistemas operativos LinuxTRANSFERMethod

 Sistemas operativos LinuxEspecifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN).

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, las operaciones de transferencia de datos fallan.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Si especifica TRANSFERMETHOD=FASP en el mandato PROTECT STGPOOL o REPLICATE NODE, ese valor altera temporalmente el parámetro TRANSFERMETHOD en los mandatos DEFINE SERVER y UPDATE SERVER.

Ejemplo: actualizar un periodo de gracia de supresión para un servidor

Actualice la definición de SERVER2 para especifica que los objetos permanecen en el servidor de destino durante 10 días, después de que se hayan marcado para la supresión.

```
update server server2 delgraceperiod=10
```

Ejemplo: actualizar el URL de un servidor

Actualizar la definición NEWSERVER para especificar que su dirección URL sea http://newserver:1580/.

```
update server newserver url=http://newserver:1580/
```

Ejemplo: Actualizar todos los servidores para comunicarse con el servidor IBM Spectrum Protect utilizando la seguridad de sesión estricta.

Actualice la definición de todos los servidores para utilizar la configuración de seguridad más estricta para autenticarse en IBM Spectrum Protect.

```
update server * sessionsecurity=strict
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE SERVER

Mandato	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

UPDATE SERVERGROUP (Actualizar una descripción de grupo de servidores)

Utilice este mandato para actualizar la descripción de un grupo de servidores.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-UPDate SERVERGroup--nombre_grupo----->
```

```
>--DEScRiption--===--descripci3n----->><
```

Parámetros

nombre_grupo (Obligatorio)
Especifica el grupo de servidores que se actualiza.

DEScRiption (Obligatorio)
Especifica una descripción del grupo de servidores. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

Ejemplo: Actualizar la descripción de un grupo de servidores

Actualizar la descripción del grupo de servidores denominado WEST_COMPLEX por "Western Region Complex".

```
update servergroup west_complex  
description="western region complex"
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE SERVERGROUP

Mandato	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.

UPDATE SPACETRIGGER (Actualizar los desencadenantes de espacio)

Utilice este mandato para actualizar los valores de los desencadenantes que determinan cuándo y cómo ha de resolver el servidor las insuficiencias de las agrupaciones de almacenamiento que utilizan clases de dispositivo FILE de acceso secuencial y DISK de acceso aleatorio.

En el caso de las agrupaciones de almacenamiento con un parámetro RECLAMATIONTYPE=SNAPLOCK, no están activados los desencadenantes de espacio.

Importante: Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Se recomienda asociar cada directorio a un sistema de archivos distinto. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio añadiendo valores que representan el espacio que resta en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar inhabilitado. Si un desencadenante se inhabilita porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a habilitar el desencadenante con el siguiente mandato: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

Consulte el mandato DEFINE SPACETRIGGER para obtener más información.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Sintaxis

```
>>-UPDate SPACETriGger--STG--+-----+----->  
'-Fullpct----porcentaje-'
```



```

>--+-----+----->
  '-SPACEexpansion---porcentaje-'
>--+-----+----->
  '-EXPansionprefix---prefijo-'
>--+-----+-----<
  '-STGPOOL---nombre_agrupación_almacenamiento-'

```

Parámetros

STG (Necesario)

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

Fullpct

Este parámetro especifica el porcentaje de utilización de la agrupación de almacenamiento.

Cuando se sobrepasa este valor, el desencadenante de espacio crea nuevos volúmenes.



Puede determinar la utilización de la agrupación de almacenamiento ejecutando el mandato QUERY STGPOOL con FORMAT=DETAILED. El porcentaje de utilización de la agrupación de almacenamiento se muestra en el campo "Util. desencadenante espacio". El cálculo de este porcentaje no incluye volúmenes reutilizables potenciales. El cálculo de la utilización del porcentaje utilizado para la migración y la reclamación, no obstante, sí incluye los volúmenes reutilizables potenciales.

SPACEexpansion


Para los desencadenantes de espacio de las agrupaciones de almacenamiento de tipo FILE de acceso secuencial, este parámetro se utiliza para determinar el número de volúmenes adicionales que se crean en la agrupación de almacenamiento. Los volúmenes se crean utilizando el valor de MAXCAPACITY de la clase de dispositivo de la agrupación de almacenamiento. En desencadenantes de espacio para las agrupaciones de almacenamiento DISK de acceso aleatorio, el desencadenante de espacio crea un único volumen por medio del valor EXPANSIONPREFIX.

EXPansionprefix



Este parámetro especifica el prefijo que el servidor utiliza para crear nuevos archivos de agrupación de almacenamiento. Este parámetro es opcional y sólo se aplica a la clase de dispositivo DISK de acceso aleatorio. El prefijo predeterminado es la ruta de instalación del servidor.


El prefijo puede incluir uno o varios caracteres de separación de directorios; por ejemplo:  Sistemas operativos AIX
 Sistemas operativos Linux

```
/opt/tivoli/tsm/server/bin/
```

 Sistemas operativos Windows

```
c:\Archivos de programa\tivoli\tsm\
```

 Sistemas operativos AIX  Sistemas operativos Linux Puede especificar hasta 250 caracteres. Si especifica un prefijo que no es válido, la expansión automática podría no ejecutarse correctamente.

 Sistemas operativos Windows Puede especificar hasta 200 caracteres. Si el servidor se ejecuta como servicio de Windows, el prefijo predeterminado es el directorio c:\wnnt\system32. Si especifica un prefijo que no es válido, la expansión automática podría no ejecutarse correctamente.

Este parámetro no es válido para desencadenantes de espacio de agrupaciones de almacenamiento de acceso secuencial FILE. Los prefijos se obtienen de los directorios especificados con la clase de dispositivo asociada.

STGPOOL

Especifica la agrupación de almacenamiento asociada a este desencadenante de espacio. Si no se especifica el parámetro STGPOOL, se actualizará el desencadenante de espacio de agrupación de almacenamiento predeterminado.

Este parámetro no se aplica a las agrupaciones de almacenamiento con el parámetro RECLAMATIONTYPE=SNAPLOCK.

Ejemplo: incrementar la cantidad de espacio para una agrupación de almacenamiento

Incrementar la cantidad de espacio de una agrupación de almacenamiento un 50 por ciento cuando se alcance el 80 por ciento de utilización de los volúmenes existentes. Se creará el espacio en los directorios asociados con la clase de dispositivo.

```
update spacetrigger stg spaceexpansion=50 stgpool=file
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE SPACETRIGGER

Mandato	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.

UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)

Utilice este mandato para actualizar un umbral de supervisión de estado existente.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

Sintaxis

```
>>-UPDate STATusthreshold--nombre_umbral--+-----+>
                                     '-Activity----nombre_actividad-'

>--+-----+-----+-----+-----+-----+----->
   '-Condition--++-EXists-+-'   '-Value----valor-'
           +-GT-----+
           +-GE-----+
           +-LT-----+
           +-LE-----+
           '-Equal--'

>--+-----+-----+-----+-----+-----+-----><
   '-Status----++-Normal-+-'
           +-Warning-+
           '-Error--'
```

Parámetros

nombre_umbral (Necesario)

Especifica el nombre de umbral que desea actualizar. El nombre de no puede tener más de 48 caracteres de longitud.

actividad

Especifique este valor para cambiar la actividad para un umbral existente. Este parámetro es opcional. Especifique uno de los siguientes valores:

PROCESSSUMMARY

Especifica el número de procesos que están activos actualmente.

SESSIONSUMMARY

Especifica el número de sesiones que están activas actualmente.

CLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente que están activas actualmente.

SCHEDCLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente planificadas.

DBUTIL

Especifica el porcentaje de utilización de base de datos. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DBFREESPACE
Especifica el espacio libre disponible en la base de datos en gigabytes.

DBUSEDSPACE
Especifica la cantidad de espacio de base de datos que se utiliza, en gigabytes.

ARCHIVELOGFREESPACE
Especifica el espacio libre que está disponible en el registro de archivo, en gigabytes.

STGPOOLUTIL
Especifica el porcentaje de utilización de agrupación de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

STGPOOLCAPACITY
Especifica la capacidad de agrupación de almacenamiento en gigabytes.

AVGSTGPOOLUTIL
Especifica el porcentaje medio de utilización de agrupación de almacenamiento en todas las agrupaciones de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

TOTSTGPOOLCAPACITY
Especifica la capacidad total de agrupación de almacenamiento en gigabytes para todas las agrupaciones de almacenamiento disponibles.

TOTSTGPOOLS
Especifica el número de agrupaciones de almacenamiento definidas.

TOTRWSTGPOOLS
Especifica el número de agrupaciones de almacenamiento definidas que se puede leer o en las que se puede escribir.

TOTNOTRWSTGPOOLS
Especifica el número de agrupaciones de almacenamiento definidas que no se pueden leer o en las que no se puede escribir.

STGPOOLINUSEANDDEFINED
Especifica el número total de volúmenes definidos que se están utilizando.

ACTIVELOGUTIL
Especifica el porcentaje de utilización actual del registro activo. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

ARCHLOGUTIL
Especifica la utilización actual del registro de archivado. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

CPYSTGPOOLUTIL
Especifica el porcentaje de utilización para una agrupación de almacenamiento de copia. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

PMRYSTGPOOLUTIL
Especifica el porcentaje de utilización para una agrupación de almacenamiento primario. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DEVCLASSPCTDRVOFFLINE
Especifica el porcentaje de utilización de las unidades que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDRVPOLLING
Especifica el sondeo de unidades, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTLIBPATHSOFFLINE
Especifica las rutas de biblioteca que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTPATHSOFFLINE
Especifica el porcentaje de rutas de clase de dispositivo que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDISKSNOTRW
Especifica el porcentaje de discos que no se pueden grabar para la clase de dispositivo de disco. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDISKSUNAVAILABLE
Especifica el porcentaje de volúmenes de disco que no están disponibles, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

FILEDEVCLASSPCTSCRUNALLOCATABLE
Especifica el porcentaje de volúmenes reutilizables que el servidor no puede asignar para una determinada clase de dispositivo de archivo no compartido. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

Condition

Especifique este valor para cambiar la condición de un umbral existente. Este parámetro es opcional. Especifique uno de los siguientes valores:

EXists

Crea un indicador de supervisión de estado si existe la actividad.

GT

Crea un indicador de supervisión de estado si la salida de actividad es mayor que el valor especificado.

GE

Crea un indicador de supervisión de estado si la salida de actividad es mayor que o igual al valor especificado.

LT

Crea un indicador de supervisión de estado si la salida de actividad es menor que el valor especificado.

LE

Crea un indicador de supervisión de estado si la salida de actividad es menor que o igual al valor especificado.

EQual

Crea un indicador de supervisión de estado si la salida de actividad es igual al valor especificado.

Value

Especifique este parámetro para cambiar el valor que se compara con la salida de actividad para la condición especificada. Puede especificar un entero en el rango 0 – 999999999999999.

Status

Especifique este valor para cambiar el estado del indicador que se crea en la supervisión de estado si pasa la condición que se está evaluando. Este parámetro es opcional. Especifique uno de los siguientes valores:

Normal

Especifica que el indicador de estado tiene un valor de estado normal.

Aviso

Especifica que el indicador de estado tiene un valor de estado de aviso.

Error

Especifica que el indicador de estado tiene un valor de estado de error.

Actualizar un umbral de estado existente

Actualice un umbral de estado para el porcentaje medio de programa de utilidad de agrupación de almacenamiento emitiendo el mandato siguiente:

```
update statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=90 condition=gt status=error
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE STATUSTHRESHOLD

Mandato	Descripción
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

Utilice este mandato para cambiar una agrupación de almacenamiento.

Restricción: Si un cliente utiliza la función de escritura simultánea y la deduplicación de datos, la función de deduplicación de datos se desactiva durante el proceso de copia de seguridad en una agrupación de almacenamiento.

El mandato UPDATE STGPOOL tiene seis formatos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Mandatos relacionados con UPDATE STGPOOL

Mandato	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
MOVE MEDIA	Mueve los volúmenes de agrupaciones de almacenamiento gestionados por una biblioteca automatizada.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.

- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores en la nube)
Utilice este mandato para actualizar una agrupación de almacenamiento de contenedor en un entorno de nube. Las agrupaciones de almacenamiento en la nube no están soportadas en Linux on System z.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de directorio)
Utilice este mandato para actualizar una agrupación de almacenamiento de contenedores de directorio.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)
Utilice este mandato para actualizar una agrupación de almacenamiento de copia de contenedor.

- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso aleatorio)
Utilice este mandato para actualizar una agrupación de almacenamiento de acceso aleatorio.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso secuencial)
Utilice este mandato para actualizar una agrupación de almacenamiento de acceso secuencial.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de acceso secuencial)
Utilice este mandato para actualizar una agrupación de almacenamiento de copia de acceso secuencial.
- UPDATE STGPOOL (Actualizar un acceso secuencial de datos activos)
Utilice este mandato para actualizar una agrupación de datos activos.

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores en la nube)

Utilice este mandato para actualizar una agrupación de almacenamiento de contenedor en un entorno de nube. Las agrupaciones de almacenamiento en la nube no están soportadas en Linux on System z.

El método preferido para definir y configurar una agrupación de almacenamiento del contenedor en la nube es utilizar Centro de operaciones. Para obtener instrucciones y sugerencias para el Centro de operaciones y la interfaz de línea de mandatos, consulte la sección Configuración de una agrupación de almacenamiento de contenedor en la nube para el almacenamiento de datos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DESCRiption----descripción-'
>--+-----+-----+-----+----->
  '-CLOUDType---+Swift-----'  '-CLOUDUrl---url_nube-'
      +-Softlayer+
      '-VlSwift---'
>--+-----+----->
  |                                     (1) |
  '-IDENTity----identidad_nube-----'
>--+-----+----->
  '-PAssword---contraseña-'
>--+-----+----->
  '-CLOUDLocation---+OFFpremise+-'
      '-ONpremise--'
>--+-----+----->
  |                                     (2) |
  '-BUCKETName----nombre_grupo-----'
>--+-----+----->
  '-ACCess---+READWrite---+'
      +-READOnly----+
      +-UNAVailable+
      '-DESTroyed---'
>--+-----+----->
  '-MAXWriters---+NOLimit-----+-'
      '-máximo_grabadores-'
>--+-----+----->
  '-REUsedelay---días-'
>--+-----+-----><
  |                                     .-COMPReSSion---Yes----- |
  '-ENCRypt---+Yes-+-+-----+-'
      '-No--'  '-COMPReSSion---+Yes+-'
```

Notas:

1. Si ha especificado CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY.
2. Este parámetro solo es válido si especifica CLOUDTYPE=S3.

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que se actualiza. Este parámetro es necesario.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

CLOUDType

Especifica el tipo de entorno de nube donde está configurando una agrupación de almacenamiento. Este parámetro es opcional. Especifique uno de los siguientes valores:

SOftlayer

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing IBM® SoftLayer (IBM Bluemix) con un sistema cloud computing OpenStack Swift.

SWift

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 2 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

V1Swift

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

Restricción: Si ha utilizado el mandato DEFINE STGPOOL para definir una agrupación de almacenamiento con CLOUDTYPE=S3 (Simple Storage Service), no puede cambiar a otro tipo de nube utilizando el mandato UPDATE STGPOOL. Asimismo, no puede cambiar el tipo de nube de una agrupación de almacenamiento no S3 a S3 utilizando el mandato UPDATE STGPOOL.

CLOUDUrl

Especifica el URL del entorno de nube donde está configurando la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un URL de punto final de región, una dirección IP de aplicación de acceso, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo `https://` o `http://`, al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL no se valida hasta que empieza la primera copia de seguridad.

Para obtener más información sobre cómo encontrar estos valores, seleccione su proveedor de servicios en la nube de la lista que aparece en la página Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos.

Consejo: Para utilizar más de un acceso de IBM Cloud Object Storage, liste las direcciones IP separadas por una barra vertical (|) sin espacios intercalados, como en el ejemplo siguiente:

```
CLOUDURL=<acceso_URL1>|<acceso_URL2>|<acceso_URL3>
```

Utilice varios accesoros para mejorar el rendimiento. Si está utilizando la solución IBM SoftLayer Cloud Object Store S3, sólo se necesita un accesor.

IDentity

Especifica el ID de usuario para la nube que se ha especificado en el parámetro STGTYPE=CLOUD. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si ha especificado CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

PAssword (Obligatorio)

Especifica la contraseña para la nube especificada en el parámetro STGTYPE=CLOUD. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres. Los parámetros IDENTITY y PASSWORD no se validan hasta que empieza la primera copia de seguridad.

CLOUDLocation

Especifica la ubicación física de la nube que se especifica en el parámetro CLOUD. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

- Offpremise

- ONpremise

BUCKETName

Especifica el nombre para un grupo AWS (Amazon Web Services) o una caja fuerte IBM Cloud Object Storage que se va a utilizar con esta agrupación de almacenamiento. Los grupos AWS y las cajas fuertes de IBM Cloud Object Storage se utilizan del mismo modo que los contenedores en una agrupación de almacenamiento de contenedores en la nube. Este parámetro es opcional y sólo es válido si el tipo de nube de esta agrupación de almacenamiento es S3. Si no existe el nombre que especifica, el servidor crea un grupo o caja fuerte con el nombre especificado antes de utilizar el grupo o caja fuerte. Siga las restricciones de asignación de nombres de su proveedor de nube cuando especifique este parámetro. Revise los permisos del grupo o caja fuerte y asegúrese de que las credenciales de esta agrupación de almacenamiento tienen permiso de lectura, grabación, lista y supresión de objetos en este grupo o caja fuerte.

Restricción: No puede cambiar el grupo o caja fuerte si existen contenedores de nube en esta agrupación de almacenamiento.

ACcess

Especifica cómo acceden los nodos cliente y los procesos de servidor a la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

READWrite

Especifica que los nodos de cliente y los procesos de servidor pueden realizar operaciones de lectura y grabación en la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en la agrupación de almacenamiento.

UNAVailable

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento. Como resultado, las copias de seguridad y las restauraciones fallan para esta agrupación de almacenamiento. Puede utilizar este valor para especificar que el proveedor de servicios de nube no está disponible temporalmente.

DESTroyed

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento porque el proveedor de servicios de nube está permanentemente no disponible. Las copias de seguridad y las restauraciones fallan para esta agrupación de almacenamiento, pero los intentos de suprimir objetos y contenedores de esta agrupación de almacenamiento se completan satisfactoriamente.

MAXWriters

Especifica el número máximo de sesiones de grabación que se pueden ejecutar simultáneamente en la agrupación de almacenamiento. Especifique un número máximo de sesiones de grabación para controlar que el rendimiento de la agrupación de almacenamiento en la nube no afecte negativamente a otros recursos del sistema. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que no existe un límite de tamaño máximo para el número de grabadores que puede utilizar. Este es el valor predeterminado.

máximo_grabadores

Limita el número máximo de grabadores que puede utilizar. Especifique un número entero del 1 al 99999.

REUsedelay

Especifica el número de días que deben transcurrir después de que se hayan eliminado todas las extensiones deduplicadas de una agrupación de almacenamiento en la nube. Este parámetro controla la duración con que las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento en la nube. Cuando caduca el valor especificado para este parámetro las extensiones deduplicadas se suprimen de la agrupación de almacenamiento en la nube. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento en la nube pasado un día.

días

Puede especificar un entero en el rango 0 – 9999.

Consejo: Defina este parámetro en un valor que sea mayor que el número especificado para el mandato SET DRMDBBACKUPEXPIREDDAYS. Al establecer este parámetro en un valor superior, puede garantizar que cuando restaure la base de datos a un nivel anterior, las referencias a los archivos de la agrupación de almacenamiento seguirán siendo válidas.

ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente.

Este parámetro es opcional. El valor predeterminado depende de la ubicación física de la nube, que se especifica mediante el parámetro CLOUDLOCATION. Si la nube está fuera de las instalaciones, el servidor cifra los datos de forma predeterminada. Si la nube está en las instalaciones, el servidor no cifra los datos de forma predeterminada.

COMPReSSion

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

Ejemplo 1: actualizar una agrupación de almacenamiento en la nube para especificar un número máximo de sesiones de datos

Actualice una agrupación de almacenamiento en la nube denominada STGPOOL1 y especifique un máximo de 10 sesiones de datos.

```
update stgpool stgpool1 maxwriters=10
```

Ejemplo 2: Actualizar la descripción de una agrupación de almacenamiento de contenedor en la nube

Actualice una agrupación de almacenamiento de contenedor en la nube denominada STGPOOL2. Elimine la descripción existente de la agrupación de almacenamiento.

```
update stgpool stgpool2 cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 description=""
```

Tareas relacionadas:

Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de directorio)

Utilice este mandato para actualizar una agrupación de almacenamiento de contenedores de directorio.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DESCRiption----descripción-'
. -ACCess----READWrite-----
>--+-----+----->
  '-ACCess----+READWrite--+-'
                +-READOnly----+
                '-UNAVailable-'
. -MAXSIZe----NOLimit-----
>--+-----+----->
  '-MAXSIZe----+tamaño_máximo_archivo--+'
                '-NOLimit-----'
. -MAXWriters----NOLimit-----
>--+-----+----->
```


Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 2. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

Agrupación especificada	Resultado
No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor no almacena el archivo.
Se ha especificado una agrupación como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor almacena el archivo en la agrupación de almacenamiento que ha especificado.

Consejo: Si también especifica el parámetro NEXTstgpool, actualice una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos durante el proceso de deduplicación de datos, el servidor considera que el tamaño del proceso de deduplicación de datos es el tamaño de archivo. Si el tamaño total de todos los archivos del proceso es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

MAXWriters

Especifica el número máximo de hebras de E/S que se pueden ejecutar simultáneamente en la agrupación de almacenamiento. Especifique un número máximo de hebras de E/S para controlar el número de hebras de E/S que se graban al mismo tiempo en la agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Como práctica recomendada, utilice el valor predeterminado NOLIMIT. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que no se graba ningún número máximo de hebras de E/S en la agrupación de almacenamiento.
máximo_grabadores

Limita el número máximo de hebras de E/S que puede utilizar. Especifique un número entero del 1 al 99999.

NEXTstgpool

Especifica el nombre de una agrupación de almacenamiento secuencial primaria o de acceso aleatorio en la que se almacenan los archivos cuando la agrupación de almacenamiento de contenedores de directorio está llena. Este parámetro es opcional.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

PROTECTstgpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de destino donde se realiza la copia de seguridad de los datos cuando utiliza el mandato PROTECT STGPOOL para esta agrupación de almacenamiento. Este parámetro es opcional.

PROTECTLOCALstgpools

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor en un dispositivo local en el que se realiza la copia de seguridad de los datos. Esta agrupación de almacenamiento de copia de contenedor será una agrupación de almacenamiento de destino local cuando utilice el mandato PROTECT STGPOOL. Puede especificar un máximo de dos nombres de agrupación de almacenamiento de copia de contenedor para actualizarlos. Puede separar varios nombres con comas y sin espacios intercalados. La longitud máxima de cada nombre es de 30 caracteres. Este parámetro es opcional.

Para añadir o eliminar agrupaciones de almacenamiento de copia de contenedor, especifique los nombres de agrupación de almacenamiento de copia de contenedor a incluir. Por ejemplo, si la agrupación de almacenamiento de copia de contenedor incluye COPY1 y desea añadir COPY2, especifique PROTECTLOCALSTGPOOLS=COPY1,COPY2. Para eliminar todas las agrupaciones de almacenamiento de copia de contenedor existentes asociadas a la agrupación de almacenamiento primaria, especifique una serie nula (""). Por ejemplo, COPYSTGPOOLS="".

REUsedelay

Especifica el número de días que deben transcurrir antes de que se eliminen todas las extensiones con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio. Este parámetro controla el tiempo durante el cual las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento de contenedores de directorio. Cuando expira el período de tiempo especificado para el parámetro, las extensiones con duplicados eliminados se suprimen de la agrupación de almacenamiento de contenedores de directorio. El valor predeterminado es 1. Especifique uno de los siguientes valores:

días

Especifique un número entero del 0 al 9999.

1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento de contenedores de directorio al cabo de un día.

Consejo: Establezca este parámetro en un valor mayor que el número especificado como periodo de copia de seguridad de base de datos, para asegurarse de que las extensiones de datos continúan siendo válidas cuando restaura la base de datos a otro nivel.

ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente.

COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

Ejemplo: Actualización de una agrupación de almacenamiento para especificar un número máximo de sesiones de datos

Actualice una agrupación de almacenamiento denominada STGPOOL1 y especifique un máximo de 10 sesiones de datos.

```
update stgpool stgpool1 maxwriters=10
```

Ejemplo: Actualización de una agrupación de almacenamiento para especificar el tamaño máximo

Actualice una agrupación de almacenamiento denominada STGPOOL2. La agrupación de almacenamiento especifica el tamaño máximo de archivo que el servidor puede almacenar en la agrupación de almacenamiento en 100 megabytes.

```
update stgpool stgpool2 maxsize=100M
```







Ejemplo: Actualización de la descripción de una agrupación de almacenamiento

Actualice una agrupación de almacenamiento denominada STGPOOL3. Elimine la descripción existente de la agrupación de almacenamiento.

```
update stgpool stgpool3 description=""
```

Tabla 3. Mandatos relacionados con UPDATE STGPOOL

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY CONTAINER	Visualiza información sobre un contenedor.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.

Mandato	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsUPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows	

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)

Utilice este mandato para actualizar una agrupación de almacenamiento de copia de contenedor.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+-----+-----+----->
' -MAXSCRatch-----número-' '-DESCRiption-----descripción-'
>--+-----+-----+-----+----->
' -ACCess-----+READWrite---+'
      +-READOnly-----+
      '-UNAVailable-'
>--+-----+-----+-----+----->
' -PROTECTProcess-----número-' '-REClaim-----porcentaje-'
>--+-----+-----+-----+----->
' -RECLAIMLiMit-----+NOLimit-----+'
      '-límite_vol-'
>--+-----+-----+-----+-----<<
' -REUsedelay-----días-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de actualizar.

MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero en el rango 0 - 100000000. Si el servidor puede solicitar volúmenes reutilizables según sean necesarios, no tiene que definir cada volumen que se va a utilizar.

El valor de este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

ACCess

Especifica cómo pueden acceder a los datos de la agrupación de almacenamiento los procesos como por ejemplo la protección y la reparación de agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

READWrite

Especifica que el servidor puede leer y grabar en volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que el servidor sólo puede leer volúmenes de la agrupación de almacenamiento. El servidor puede utilizar datos de la agrupación de almacenamiento para restaurar extensiones en agrupaciones de almacenamiento de

contenedor de directorios. No se permiten operaciones que graban en la agrupación de almacenamiento de contenedor de directorios.

UNAVailable

Especifica que el servidor no puede acceder a los datos almacenados en volúmenes de la agrupación de almacenamiento.

PROTECTProcess

Especifica el número máximo de procesos paralelos que se utilizan cuando se emite el mandato PROTECT STGPOOL para copiar datos en esta agrupación desde una agrupación de almacenamiento de contenedor de directorios. Este parámetro es opcional. Especifique un valor del 1 al 20.

El tiempo que es necesario para realizar la operación de copia se puede reducir utilizando varios procesos paralelos. Sin embargo, en algunos casos, cuando se ejecutan varios procesos, uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso distinto.

Al seleccionar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de cinta, el servidor utiliza un punto de montaje y una unidad. El número de puntos de montaje y unidades disponibles depende del límite de montaje de la clase de dispositivo de la agrupación de almacenamiento y de otra actividad del servidor y del sistema.

Si utiliza la opción de vista previa en el mandato PROTECT STGPOOL, sólo se utiliza un proceso y no se necesitan puntos de montaje ni unidades.

REClaim

Especifica cuando un volumen pasa a ser seleccionable para la reclamación y la reutilización. Especifica la elegibilidad como el porcentaje de espacio de un volumen que está ocupado por las extensiones que ya no se almacenan en la agrupación de almacenamiento de contenedor de directorios. La reclamación mueve cualesquiera extensiones que sigan almacenadas en la agrupación de almacenamiento de contenedor de directorios de volúmenes elegibles a otros volúmenes. La reclamación se produce sólo cuando un mandato PROTECT STGPOOL almacena datos en esta agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero en el rango 1 - 100. El valor 100 especifica que los volúmenes de esta agrupación de almacenamiento no se reclaman.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Al establecer un valor de reclamación de 50 o superior, los datos que se mueven de dos volúmenes reclamados no utilizan más del equivalente de un nuevo volumen.

Tenga cuidado al utilizar la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Por lo tanto, para fines de recuperación ante siniestro, asegúrese de que planifica las copias de seguridad de bases de datos para que se ejecuten después de que se hayan ejecutado las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM, y asegúrese de que todos los volúmenes de copia de seguridad de bases de datos se trasladen fuera del local junto con los volúmenes de DRM.

Consejo: Establezca diferentes valores de reclamación para las agrupaciones de almacenamiento de copia de contenedor fuera del local y dentro del local. Debido a que las agrupaciones de almacenamiento de copia de contenedor almacenan datos de eliminación de duplicados, las extensiones de datos abarcan varios volúmenes de cinta. Cuando seleccione un umbral de reclamación para una copia fuera del local, tenga en cuenta el número de puntos de montaje disponibles y el número de volúmenes de cinta que debe recuperar en caso de siniestro. Establecer un umbral más alto, significa que se deberán recuperar más volúmenes que si se establece la reclamación en un valor inferior. Si se utiliza un umbral más bajo se reduce el número de puntos de montaje necesarios en caso de siniestro. El método preferido consiste en definir el valor de reclamación para copias externas en 60 y, para copias internas, en el intervalo 90 - 100.

RECLAIMLimit

Especifica el número máximo de volúmenes que reclama el servidor cuando se emite el mandato PROTECT STGPOOL y se especifican las opciones RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED. Este parámetro solo es válido para las agrupaciones de almacenamiento de copia de contenedor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

NOLimit

Especifica que todos los volúmenes de la agrupación de almacenamiento de copia de contenedor se procesen para la reclamación.

límite_vol

Especifica el número máximo de volúmenes de la agrupación de almacenamiento de copia de contenedor que se reclaman. El valor que se especifique determinará cuántas nuevas cintas reutilizables están disponibles una vez completado el proceso de reclamación. Puede especificar un número comprendido entre 1 y 100000.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todas las extensiones de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva al estado reutilizable. Este parámetro es opcional. Puede especificar un entero en el rango 0 – 9999. Un valor de 0 significa que un volumen se puede volver a grabar o devolver al estado reutilizable tan pronto como se han suprimido todas las extensiones del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a extensiones de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. Si utiliza gestor recuperación ante siniestro, el número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

Ejemplo: Actualizar una agrupación de almacenamiento de copia de contenedor para retardar 30 días la reutilización de volumen

Actualizar la agrupación de almacenamiento llamada CONTAINER1_COPY2 para cambiar el retardo de la reutilización de volumen a 30 días.

```
update stgpool container1_copy2 reusedelay=30
```

Ejemplo: actualizar una agrupación de almacenamiento de copia de contenedor para limitar el número de volúmenes de cintas reclamados a 10

Actualice la agrupación de almacenamiento denominada CONTAINER1_COPY2 para cambiar el límite de reclamación a 10 volúmenes.

```
update stgpool container1_copy2 reclaimlimit=10
```

Tabla 1. Mandatos relacionados con UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)

Mandato	Descripción
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (contenedor de directorios)	Actualizar una agrupación de almacenamiento de contenedores de directorios.

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso aleatorio)

Utilice este mandato para actualizar una agrupación de almacenamiento de acceso aleatorio.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DEScRiption----descripción-'
>--+-----+----->
  '-ACCess----+--READWrite----+'
```

```

+-ReadOnly-----+
'-UNAVailable-'

>+-----+----->
'-MAXSize-----+tamaño_máximo_archivo+-'
'-NOLimit-----'

>+-----+----->
'-CRCDATA-----+Yes+-'
'-No--'

>+-----+----->
'-NEXTstgpool----nombre_agrupación-'

>+-----+-----+----->
'-Highmig----percent-' '-Lowmig----percent-'

>+-----+-----+----->
'-CACHe-----+Yes+-' '-MIGPRocess----number-'
'-No--'

>+-----+-----+----->
'-MIGDelay----días-' '-MIGContinue----+Yes+-'
'-No--'

>+-----+----->
'-AUTOCopy----+None-----+'
'+CLient-----+
'+MIGRation+
'-All-----'

>+-----+----->
| .-,-----|
| V | |
'-COPYSTGpools-----nombre_agrupación_copia+-'

>+-----+----->
'-COPYContinue----+Yes+-'
'-No--'

>+-----+----->
| .-,-----|
| V | |
'-ACTIVEDATApools-----nombre_agrupación_datos_activos+-'

.-SHRED----0-----
>+-----+-----><
'-SHRED----recuento_sobregabación-'

```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que se actualiza. Este parámetro es necesario.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los siguientes valores:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

tamaño_máximo_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Consulte la tabla siguiente para obtener información sobre dónde se almacena un archivo cuando su tamaño excede el parámetro MAXSIZE.

Tabla 1. Dónde se almacena un archivo según el tamaño del archivo y la agrupación especificada

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Si especifica el siguiente parámetro de agrupación de almacenamiento, defina una agrupación de almacenamiento de la jerarquía para que no tenga límite acerca del tamaño máximo de archivo. Al no tener ningún límite sobre el tamaño como mínimo en una agrupación, se garantiza que el servidor puede almacenar el archivo al margen de su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se produce una carga general adicional para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

NEXTSTGPOOL

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. Este parámetro es opcional.

Para suprimir de la jerarquía de almacenamiento una agrupación de almacenamiento definida anteriormente, especifique una serie nula ("") para este valor.

Si no especifica ninguna agrupación de almacenamiento siguiente, se producen las acciones siguientes:

- El servidor no puede migrar los archivos de esta agrupación de almacenamiento
- El servidor no puede almacenar archivos que superen el tamaño máximo de esta agrupación de almacenamiento en otra agrupación de almacenamiento

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

HIGHMIG

Especifica que el servidor inicia la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 100.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por nodo, a la siguiente agrupación de almacenamiento, según se ha definido con el parámetro NEXTSTGPOOL. Puede especificar HIGHMIG=100 para impedir que se produzca la migración en esta agrupación de almacenamiento.

LOWMIG

Especifica que el servidor detiene la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Puede especificar un entero del 0 al 99 para este parámetro opcional.

Cuando la migración se realiza por nodo o espacio de archivos, en función de la proximidad, el nivel de ocupación de la agrupación de almacenamiento puede caer por debajo del valor que ha especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0.

CACHE

Especifica si el proceso de migración deja una copia en caché de un archivo en esta agrupación de almacenamiento una vez migrado el archivo a la siguiente agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

Yes

Especifica que está activada la función de caché.

No

Especifica que está desactivada la función de caché.

Si se utiliza la función de caché se puede mejorar la posibilidad de recuperar archivos, pero puede afectar al rendimiento de otros procesos.

MIGPROCESS

Especifica el número de procesos que se utilizan para migrar los archivos de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero del 1 al 999.

Durante la migración, estos procesos se ejecutan en paralelo para proporcionar el potencial de mejorar los índices de migración.

Consejos:

- El número de procesos de migración depende de los siguientes valores:
 - El valor del parámetro MIGPROCESS
 - El valor de proximidad de la agrupación siguiente
 - El número de nodos o el número de grupos de proximidad con datos en la agrupación de almacenamiento que se está migrando

Para este ejemplo, `MIGPROCESS =6`, el parámetro `COLLOCATE` de la siguiente agrupación es `NODE`, pero hay solo dos nodos con datos en la agrupación de almacenamiento. El proceso de migración consta solo de dos procesos, no de seis. Si el parámetro `COLLOCATE` es el grupo `GROUP` y ambos nodos están en el mismo grupo, el proceso de migración consta solamente de un proceso. Si el parámetro `COLLOCATE` es `NO` o el grupo `FILESPACE`, y cada nodo tiene dos espacios de archivos con datos de copia de seguridad, el proceso de migración consta solamente de cuatro procesos.

- Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Para calcular un valor para comparar con el valor `MIGDELAY` especificado, el servidor cuenta los elementos siguientes:

- El número de días que el archivo ha estado en la agrupación de almacenamiento
- El número de días, si hay alguno, desde que un cliente recuperó el archivo

El menor de ambos valores se compara con el valor de `MIGDELAY` especificado. Por ejemplo, si se cumplen todas las condiciones siguientes, no se migrará un archivo:

- Un archivo ha permanecido en una agrupación de almacenamiento durante cinco días.
- Un cliente ha accedido al archivo en los tres últimos días.
- El valor especificado para el parámetro `MIGDELAY` es cuatro días.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración.

Si desea que el servidor cuente el número de días basándose tan solo en el momento en que se almacenó un archivo y no en el momento en el que se recuperó, utilice la opción del servidor `NORETRIEVEDATE`.

MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

AUTOCopy

Especifica cuándo IBM Spectrum Protect ejecuta operaciones de grabación simultáneamente en las agrupaciones de almacenamiento de copia y activas. Este parámetro afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPOOLS. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPOOLS.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea está inhabilitada.

CLient

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Para agregar o eliminar una o varias agrupaciones de almacenamiento de copia, especifique el nombre de las agrupaciones que desee incluir en la lista actualizada. Por ejemplo, si la lista de agrupaciones de almacenamiento de copia incluye COPY1 y COPY2 y desea añadir COPY3, especifique COPYSTGPOOLS=COPY1,COPY2,COPY3. Para eliminar todas las agrupaciones de almacenamiento de copia existentes asociadas con la agrupación de almacenamiento de copia principal, especifique una serie nula ("") para el valor (por ejemplo, COPYSTGPOOLS="").

Al especificar un valor para el parámetro COPYSTGPOOLS, también puede especificar un valor para el parámetro COPYCONTINUE. Si desea obtener más información, consulte el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia en las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricciones: No se admite la función de grabación simultánea en las siguientes operaciones de almacenamiento:

- Cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
- Operaciones de copias de seguridad de NAS. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia:
 - Las agrupaciones de almacenamiento de copia se ignoran
 - Los datos solo se almacenan en la agrupación de almacenamiento primaria

Atención: La función que proporciona el parámetro COPYSTGPools no tiene como finalidad sustituir el mandato BACKUP STGPool. Si utiliza el parámetro COPYSTGPools, continúe utilizando el mandato BACKUP STGPool para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPools. Este parámetro es opcional. Cuando se especifica el parámetro COPYCONTINUE, debe existir una lista COPYSTGPools o especificarse también el parámetro COPYSTGPools.

Puede especificar los valores siguientes:

Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEDATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPools y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro solamente está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos "NATIVE" o "NONBLOCK". Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - o NETAPPDUMP
 - o CELERRADUMP
 - o NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria especificada en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos:
 - o Las agrupaciones de datos activos se ignoran
 - o Los datos solo se almacenan en la agrupación de almacenamiento primaria
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el mandato COPY ACTIVE DATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVE DATA POOLS no tiene como finalidad sustituir al mandato COPY ACTIVE DATA. Si utiliza el parámetro ACTIVE DATA POOLS, utilice el mandato COPY ACTIVE DATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

SHRED

Especifica si los datos se van a sobregrabar físicamente cuando se supriman. Este parámetro es opcional. Puede especificar un entero del 0 al 10.

Si especifica un valor de cero, el servidor suprime los datos de la base de datos. Sin embargo, el almacenamiento que se utiliza para contener los datos no se sobregraba, y los datos existirán en el almacenamiento hasta que se reutilice el almacenamiento para otros datos. Los datos se podrían descubrir y reconstruir tras haberlos suprimido. Si se cambia el valor (por ejemplo, se restablece en 0) no afecta a los datos que ya se han suprimido y están a la espera de sobregrabarse.

Si especifica un valor superior a 0, el servidor suprime los datos lógicamente y físicamente. El servidor sobregraba el almacenamiento utilizado para contener los datos el número especificado de veces. Esta sobregrabación aumenta la dificultad de descubrir y reconstruir los datos tras su supresión.

Para asegurarse de que todas las copias de los datos se destruyen, especifique un valor SHRED superior a cero para la agrupación de almacenamiento especificada en el parámetro NEXT STG POOL. No especifique ni COPY STG POOLS ni ACTIVE DATA POOLS. Normalmente la especificación de valores relativamente altos para el recuento de sobregrabación mejora el nivel de seguridad, pero podría afectar negativamente al rendimiento.

La sobregrabación de datos suprimidos se realiza de forma asíncrona tras completarse la operación de supresión. Por lo tanto, el espacio ocupado por los datos suprimidos permanecerá ocupado durante algún tiempo. El espacio no está disponible como espacio libre para nuevos datos.

No se puede utilizar un valor SHRED superior a cero si el valor del parámetro CACHE es YES. Si desea habilitar la destrucción de datos para una agrupación de almacenamiento existente para la que ya está habilitada la función de caché, debe cambiar el valor del parámetro CACHE a NO. Los archivos en caché existentes permanecerán en el almacenamiento, de forma que las posteriores solicitudes de recuperación se puedan cumplir rápidamente. Si se necesita espacio para almacenar datos nuevos, se borrarán los archivos en caché existentes de modo que el espacio que han ocupado pueda utilizarse para datos nuevos. Los archivos en caché existentes no se destruyen cuando se borran.

Importante: Después de que haya finalizado una operación de exportación y se hayan identificado los archivos para la exportación, los cambios que se realicen en el valor SHRED se ignorarán. Una operación de exportación que se ha suspendido retiene el valor de SHRED original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor SHRED de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el mandato de exportación después de realizar la operación de limpieza necesaria.

Ejemplo: actualizar una agrupación de almacenamiento de acceso aleatorio para permitir la función de caché

Actualizar la agrupación de almacenamiento denominada BACKUP POOL que es aleatoria para permitir la función de caché cuando el servidor migra los archivos a la siguiente agrupación de almacenamiento.

```
update stgpool backuppool cache=yes
```

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso secuencial)

Utilice este mandato para actualizar una agrupación de almacenamiento de acceso secuencial.

Restricciones:

1. No es posible utilizar este mandato para cambiar el formato de datos de una agrupación de almacenamiento.
2. Si el valor de DATAFORMAT es NETAPPDUMP, CELERRADUMP o NDMPDUMP, sólo puede modificar los atributos siguientes:
 - o DESCRIPTION
 - o ACCESS
 - o COLLOCATE
 - o MAXSCRATCH
 - o REUSEDELAY

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DESCription---descripción-'
>--+-----+----->
  '-ACCess---+READWrite---+-'
      +-READOnly-----+
      '-UNAVailable-'
>--+-----+----->
  |                                     (1) (2) |
  '-MAXSize---+tamaño_máximo_archivo+-----'
      '-NOLimit-----'
>--+-----+----->
  |                                     (1) |
  '-CRCData---+Yes+-----'
      '-No--'
>--+-----+----->
  |                                     (1) (2) |
  '-NEXTstgpool---pool_name-----'
>--+-----+----->
  |                                     (1) (2) |
  '-HIghmig---percent-----'
>--+-----+----->
  |                                     (1) (2) |
  '-LOWmig---percent-----'
>--+-----+----->
  |                                     (1) (2) |
  '-REClaim---porcentaje-----'
>--+-----+----->
  |                                     (1) (2) |
  '-RECLAIMProcess---number-----'
>--+-----+----->
  |                                     (1) (2) |
  '-RECLAIMSTGpool---pool_name-----'
>--+-----+----->
  |                                     (2) |
  '-COLlocate---+No-----'
      +-GRoup-----+
```


Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

tamaño_máximo_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
----------------------	-------------------------	-----------

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSize=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. No puede migrar datos de una agrupación de almacenamiento de acceso secuencial a una agrupación de almacenamiento de acceso aleatorio. Este parámetro es opcional. La siguiente agrupación de almacenamiento debe ser una agrupación de almacenamiento primaria.

Para suprimir un valor existente, especifique una serie nula ("").

Si esta agrupación de almacenamiento no tiene una agrupación de almacenamiento que le siga, el servidor no puede migrar los archivos de esta agrupación de almacenamiento y no puede almacenar en otra agrupación de almacenamiento los archivos que sobrepasan el tamaño máximo de esta agrupación de almacenamiento.

Cuando no hay suficiente espacio disponible en la agrupación de almacenamiento actual, el parámetro NEXTSTGPOOL para las agrupaciones de almacenamiento de acceso secuencial no permite que los datos se almacenen en la agrupación siguiente. En este caso, el servidor emite un mensaje y la transacción no se efectúa correctamente.

Para las siguientes agrupaciones de almacenamiento con un tipo de dispositivo FILE, el servidor realiza una comprobación preliminar para determinar si hay disponible espacio suficiente. Si no hay espacio disponible, el servidor salta a la siguiente agrupación de almacenamiento de la jerarquía. Si hay espacio disponible, el servidor intenta almacenar datos en esa agrupación. No obstante, es posible que falle la operación de almacenamiento porque cuando se intenta realmente realizar la operación de almacenamiento el espacio ya no está disponible.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor de nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.
- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP

HIghmig

Especifica que el servidor inicia la migración cuando la utilización de la agrupación de almacenamiento alcanza este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 100.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por volumen, a la siguiente agrupación de almacenamiento definida para la agrupación de almacenamiento. Puede establecer el umbral superior de migración en 100 para impedir la migración en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

LOwmig

Especifica que el servidor detiene la migración cuando la utilización de la agrupación de almacenamiento es igual o inferior a este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 99.

Cuando la agrupación de almacenamiento alcanza el umbral inferior de migración, el servidor no inicia la migración de los archivos de otro volumen. Puede establecer el umbral inferior de migración en 0 para permitir que la migración vacíe la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

REClaim



Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible

para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

 Sistemas operativos AIX  Sistemas operativos Windows Para las agrupaciones de almacenamiento que utilizan dispositivos WORM, se puede bajar el valor predeterminado 100. Al bajar el valor, el servidor puede consolidar los datos en menos volúmenes cuando sea necesario. Los volúmenes que se vacían por la operación de reclamación se pueden dar de baja de la biblioteca, con lo que quedan ranuras libres para nuevos volúmenes. Los volúmenes no se pueden reutilizar porque son de una sola operación de grabación.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento primaria de acceso secuencial.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que no se ha especificado el parámetro RECLAIMSTGPPOOL o que la agrupación de almacenamiento de reclamación tiene la misma clase de dispositivo que la agrupación de almacenamiento que se reclama, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMSTGpool

Especifica otra agrupación de almacenamiento primaria como destino de los datos reclamados de esta agrupación de almacenamiento. Este parámetro es opcional. Cuando el servidor reclama volúmenes para la agrupación de almacenamiento, los datos sin caducar de los volúmenes que se están reclamando se traspasan a la agrupación de almacenamiento indicada en este parámetro.

Para suprimir un valor existente, especifique una serie nula ("").

Una agrupación de almacenamiento de reclamación tiene la mayor utilidad para una agrupación de almacenamiento que sólo tenga una unidad en su biblioteca. Al especificar este parámetro, el servidor traspasa todos los datos de los volúmenes reclamados a la agrupación de almacenamiento de reclamación independientemente del número de unidades de la biblioteca.

Para volver a traspasar los datos de la agrupación de almacenamiento de reclamación a la agrupación de almacenamiento original, utilice la jerarquía de agrupaciones de almacenamiento. Especifique la agrupación de almacenamiento original como la siguiente agrupación de almacenamiento de la agrupación de almacenamiento de reclamación.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario. La función de proximidad también pueden afectar al número de procesos que migran discos a agrupación secuencial.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada. Durante la migración de disco, los procesos se crean a un nivel de espacio de archivos.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Se recomienda utilizar cintas cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para nodos agrupados, y en el nivel de nodo para nodos no agrupados.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos que se denominan A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para espacios de archivos agrupados.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODe

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios

de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Para COLLOCATE=NODE, el servidor crea procesos en el nivel de nodo cuando se migran datos del disco.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

Para COLLOCATE=FILESPACE, el servidor crea procesos en el nivel de espacio de archivos al migrar datos del disco.

MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables, se evita tener que definir cada volumen que se va a utilizar.

El valor especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Cuando se suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Al especificar este parámetro, puede asegurarse de que la base de datos se pueda restaurar a un nivel anterior y que las referencias de base de datos a los archivos de la agrupación de almacenamiento todavía sean válidas.

OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el mandato MOVE MEDIA. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Todos los archivos de un volumen deben poder seleccionarse para una operación de migración antes de que el servidor seleccione el volumen para migración. Para calcular un valor para comparar con el valor MIGDELAY especificado, el servidor cuenta el número de días que el archivo ha permanecido en la agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999.

Si desea que el servidor cuente el número de días sólo basándose en el momento en que se almacenó un archivo y no en el momento en que se recuperó, utilice la opción del servidor NORETRIEVEDATE.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no han estado almacenados en la agrupación de almacenamiento el número de días que especifica el período de retardo de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra los archivos si no han estado almacenados en la agrupación de almacenamiento el número de días que especifica el período de retardo de migración.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGProcess

Especifica el número de procesos paralelos que se utilizará para migrar los archivos de los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta el número de agrupaciones de almacenamiento secuenciales que participarán en la migración y el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la migración.

Por ejemplo, supongamos que desea migrar los volúmenes de dos agrupaciones de almacenamiento secuencial primarias simultáneamente y que desea especificar tres procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que la agrupación de almacenamiento a la que se están migrando los archivos tienen la misma clase de dispositivo que la agrupación de almacenamiento de la que se migran, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una unidad corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar simultáneamente seis procesos de migración, necesita como mínimo un total de 12 puntos de montaje y 12 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 12 como mínimo.

Si el número de procesos de migración especificados es mayor que el número de puntos de montaje o unidades disponibles, los procesos que no obtengan puntos de montaje o unidades esperarán a que haya puntos de montaje o unidades disponibles. Si las unidades o los puntos de montaje no pasan a estar disponibles dentro del tiempo MOUNTWAIT, los procesos de migración finalizarán. Para obtener información acerca de la especificación del tiempo MOUNTWAIT, consulte el apartado DEFINE DEVCLASS (Definir una clase de dispositivo).

El servidor de IBM Spectrum Protect iniciará el número especificado de procesos de migración independientemente del número de volúmenes elegibles para la migración. Por ejemplo, si especifica diez procesos de migración y sólo seis volúmenes son elegibles para migración, el servidor iniciará diez procesos y cuatro de ellos terminarán sin que se procesen volúmenes.

Nota: Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. Este parámetro afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si la opción AUTOCOPY se establece en ALL o CLIENT y existe como mínimo una agrupación de almacenamiento que aparece listada en las opciones COPYSTGPOOLS o ACTIVEATAPOOLS, la eliminación de duplicados del lado del cliente está inhabilitada.

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPOOLS. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEATAPOOLS.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea esta inhabilitada.

CLient

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Para agregar o eliminar una o varias agrupaciones de almacenamiento de copia, especifique el nombre de las agrupaciones que desee incluir en la lista actualizada. Por ejemplo, si la lista de agrupaciones de almacenamiento de copia incluye COPY1 y COPY2 y desea añadir COPY3, especifique COPYSTGPOOLS=COPY1,COPY2,COPY3. Para eliminar todas las agrupaciones de almacenamiento de copia existentes asociadas con la agrupación de almacenamiento de copia principal, especifique una serie nula ("") para el valor (por ejemplo, COPYSTGPOOLS="").

Al especificar un valor para el parámetro COPYSTGPOOLS, también puede especificar un valor para el parámetro COPYCONTINUE. Si desea obtener más información, consulte el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - NETAPPDUMP
 - CELERRADUMP
 - NDMPDUMP
2. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se da soporte a la grabación simultánea en las siguientes operaciones de almacenamiento. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia, éstas se pasarán por alto y los datos se almacenarán únicamente en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.

Atención: La función que proporciona el parámetro COPYSTGPOOLS no tiene como finalidad sustituir el mandato BACKUP STGPOOL. Si utiliza el parámetro COPYSTGPOOLS, continúe utilizando el mandato BACKUP STGPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOOLS. Este parámetro es opcional. El valor predeterminado es YES. Cuando se especifica el parámetro COPYCONTINUE, debe existir una lista COPYSTGPOOLS o especificarse también el parámetro COPYSTGPOOLS.

El parámetro COPYCONTINUE no afecta a la función de grabación simultánea durante la migración.

Puede especificar los siguientes valores:

Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro `ACTIVEDATAPOOLS` es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros `COPYSGTPOOLS` y `ACTIVEDATAPOOLS` no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento principal a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos `NATIVE` o `NONBLOCK`. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
 - `NETAPPDUMP`
 - `CELERRADUMP`
 - `NDMPDUMP`
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria que se ha especificado en `TOCDESTINATION` en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos, éstas se pasarán por alto y los datos sólo se almacenarán en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento `CENTERA`.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el mandato `COPY ACTIVE DATA` para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro `ACTIVEDATAPOOLS` no tiene como finalidad sustituir al mandato `COPY ACTIVE DATA`. Si utiliza el parámetro `ACTIVEDATAPOOLS`, utilice el mandato `COPY ACTIVE DATA` para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo `FILE`.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo asociada al tipo de dispositivo `FILE`. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato `QUERY PROCESS` para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

Ejemplo: actualizar los volúmenes reutilizables que pueden montarse de la agrupación de almacenamiento primaria secuencial

Actualice la agrupación de almacenamiento secuencial primaria que se denomina `TAPEPOOL1` para permitir que se monten 10 volúmenes reutilizables como máximo.

```
update stgpool tapepool1 maxscratch=10
```

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de acceso secuencial)

Utilice este mandato para actualizar una agrupación de almacenamiento de copia de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>+-----+
  '-DESCRiption----descripción-'
>+-----+
  '-ACCess---+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>+-----+
  '-COLlocate---+No-----+'
      +-GRoup-----+
      +-NODE-----+
      '-Filespace-'
>+-----+-----+-----+-----+-----+
  '-REClaim----porcentaje-' '-RECLAIMProcess----number-'
>+-----+-----+-----+-----+-----+
  '-OFFSITERECLAIMLimit---+NOLimit--+'
      '-número--'
>+-----+-----+-----+-----+-----+
  '-MAXSCRatch----número-' '-REUsedelay----dias-'
>+-----+-----+-----+-----+-----+
  '-OVFLocation----ubicación-' '-CRCDData---+Yes--+'
      '-No--'
>+-----+-----+-----+-----+-----+
  '-DEDUPlicate---+No-----+'
      | (1) |
      '-Yes-----'
>+-----+-----+-----+-----+-----+<<
  | (2) |
  '-IDENTIFYProcess----número-----'
```

Notas:

1. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
2. Este parámetro sólo está disponible si el valor del parámetro DEDUPLICATE es YES.

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de copia que se ha de actualizar.

DESCRiption

Especifica la descripción de la agrupación de almacenamiento de copia. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor acceder a los archivos de la agrupación de almacenamiento de copia. Este parámetro es opcional. Puede especificar los valores siguientes:

READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de almacenamiento de copia.

READOnly

Especifica que los nodos cliente sólo puedan leer archivos que están almacenados en los volúmenes en la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes activos de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor 100 significa que no se realizará la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado 100, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de copia que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación de almacenamiento de copia o primaria que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de almacenamiento de copia original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de almacenamiento de copia.

RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para cada agrupación de almacenamiento debe tener un límite de montaje de ocho como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento de copia. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de copia de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, suponga que una agrupación de almacenamiento de copias contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclamarán los tres volúmenes cuando se ejecute la reclamación. Si se especifica un valor de 2, sólo se reclamarán VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclamará VOL1.

MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se ha especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento de copia y la capacidad correspondiente estimada para la agrupación de almacenamiento de copia.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de almacenamiento de copia mientras no se cambie la modalidad de acceso. Un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor de IBM Spectrum Protect no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento de copia seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el mandato MOVE MEDIA. Este parámetro es opcional. El nombre de

ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

CRCData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T1000C y T1000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

Ejemplo: actualizar una agrupación de almacenamiento de copia para una reutilización de volumen 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente

Actualizar la agrupación de almacenamiento de copia que se denomina TAPEPOOL2 de modo que el retardo de reutilización de volúmenes se cambie por 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente.

```
update stgpool tapepool2 reusedelay=30 collocate=node
```

Referencia relacionada:

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

UPDATE STGPOOL (Actualizar un acceso secuencial de datos activos)

Utilice este mandato para actualizar una agrupación de datos activos.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>+-----+-----+----->
  '-DESCRiption---descripción-'
>+-----+-----+----->
  '-ACCess---+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>+-----+-----+----->
  '-COLlocate---+No-----+'
      +-GRoup-----+
      +-NODE-----+
      '-Filespace-'
>+-----+-----+----->
  '-REClaim---porcentaje-' '-RECLAIMPRocess---number-'
>+-----+-----+----->
  '-OFFSITERECLAIMLimit---+NOLimit-+-'
      '-número--'
>+-----+-----+----->
  '-MAXSCRatch---número-' '-REUsedelay---días-'
>+-----+-----+----->
  '-OVFLocation---ubicación-' '-CRCDData---+Yes-+-'
      '-No--'
>+-----+-----+----->
  '-DEDUPlicate---+No-----+'
      |      (1) |
      '-Yes-----'
>+-----+-----+-----><
  |      (2) |
  '-IDENTIFYPRocess---número-----'
```

Notas:

1. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
2. Este parámetro sólo está disponible si el valor del parámetro DEDUPLICATE es YES.

Parámetros

nombre_agrupación (Obligatorio)

Especifica el nombre de la agrupación de datos activos que se ha de actualizar.

DESCRiption

Especifica una descripción de la agrupación de datos activos. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, reclamación) pueden acceder a los archivos de la agrupación de datos activos. Este parámetro es opcional. Puede especificar los siguientes valores:

READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de datos activos.

READOnly

Especifica que los nodos cliente pueden leer sólo los archivos que están almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar las versiones activas de los archivos de copia de seguridad en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar las versiones activas de los archivos de copia de seguridad en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación produce que el espacio fragmentado y el espacio que ocupan los archivos de copia de seguridad inactivos en los volúmenes pueda volver a utilizarse traspasando los restantes archivos no caducados y los archivos de copia de seguridad activos desde un volumen hasta otro volumen. Esta acción hace que el volumen original esté disponible para su reutilización. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor 100 significa que no se realizará la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, que es 60, especifique un valor que represente, como mínimo, el 50 % para que los archivos almacenados en dos volúmenes puedan combinarse en un único volumen de salida.

Cuando un volumen de agrupación de datos activos que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación primaria o de datos activos que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de datos activos original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de datos activos.

RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para cada agrupación de almacenamiento debe tener un límite de montaje de ocho como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de datos activos. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de datos activos de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, imaginemos que una agrupación de datos activos contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclaman los tres volúmenes cuando se ejecuta la reclamación. Si especifica un valor de 2, sólo se reclaman VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclama VOL1.

MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se especifica para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de datos activos y la capacidad correspondiente estimada para la agrupación de datos activos.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprime de la agrupación de datos activos mientras no se cambie la modalidad de acceso. Un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor de IBM Spectrum Protect no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de datos activos seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el mandato MOVE MEDIA. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

CRCData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los mandatos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del mandato QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.




Ejemplo: actualizar una agrupación de datos activos

Actualizar la agrupación de datos activos que se denomina TAPEPOOL2 de modo que el retardo de reutilización de volúmenes se cambie por 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente.

```
update stgpool tapepool3 reusedelay=30 collocate=node
```

Referencia relacionada:

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

UPDATE STGPOOLDIRECTORY (Actualización de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para actualizar un directorio de agrupaciones de almacenamiento.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

Sintaxis

```
>>-UPDate STGPOOLDIrectory--nombre_agrupación--directorio----->
                                     .-MAXProcess-----4-----.
>---ACcess-----+-READWrite---+-----+-----+----->
      +-READOnly-----+   '-MAXProcess-----número-'
      +-DEStroyed---+
      '-UNAVailable-'

      .-Wait-----No-----.
>---+-----+-----+-----><
      '-Wait-----+No---+'
      '-Yes-'
```

Parámetros

nombre_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que contiene el directorio que se debe actualizar. Este parámetro es necesario.

directorio (Obligatorio)

Especifica un directorio del sistema de archivos de la agrupación de almacenamiento. Este parámetro es necesario.

ACcess (Obligatorio)

Especifica la forma en que los nodos cliente y los procesos del servidor pueden acceder a los archivos en el directorio de agrupaciones de almacenamiento. Este parámetro es necesario. Son posibles los siguientes valores:

READWrite

Especifica que los archivos se pueden leer desde un directorio de agrupaciones de almacenamiento y grabarse en él.

READOnly

Especifica que los archivos se pueden leer desde el directorio de agrupaciones de almacenamiento.

DEStroyed

Especifica que los archivos están dañados de forma permanente y se deben destruir en el directorio de agrupaciones de almacenamiento. Utilice esta modalidad de acceso para indicar que se debe recuperar un directorio completo de agrupaciones de almacenamiento.

Consejos:

- Marque los directorios de agrupaciones de almacenamiento como `DESTROYED` antes de realizar la recuperación de datos. Cuando el directorio de agrupaciones de almacenamiento se marca como destruido, puede recuperar extensiones de datos en el servidor de réplica de destino.
- Utilice el parámetro `MAXPROCESS` para especificar el número de procesos paralelos que se pueden utilizar para actualizar un directorio de agrupaciones de almacenamiento.

UNAVailable

Especifica que no se puede acceder a los archivos en el directorio de agrupaciones de almacenamiento.

MAXProcess

Especifica el número máximo de procesos paralelos que utilizar para actualizar un directorio de agrupaciones de almacenamiento. Este parámetro es opcional. Puede especificar un valor comprendido entre 1 y 99. El valor predeterminado es 4.

Restricción: Sólo puede utilizar este parámetro cuando se especifica el parámetro `ACCESS=DESTROYED`.

Si especifica el parámetro `ACCESS=DESTROYED`, cada contenedor del directorio de agrupaciones de almacenamiento se actualiza por medio de un proceso. Si el número máximo de procesos paralelos es mayor o igual que el número de contenedores que hay que actualizar, solo se crea un proceso para cada contenedor. Si el número de contenedores supera el valor del parámetro `MAXPROCESS`, el mandato espera a que los mandatos hijo finalicen para poder iniciar nuevos procesos.

Wait

Este parámetro opcional especifica si se ha de esperar a que el servidor de IBM Spectrum Protect complete el proceso de este mandato de forma subordinada. El valor predeterminado es `NO`. Puede especificar los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Yes

El servidor procesa este mandato de forma subordinada. La operación debe haber terminado su proceso para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del

servidor o en ambas, en función de dónde se anoten los mensajes.
 Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: Actualización de un directorio de agrupaciones de almacenamiento para destruirlo

Actualice un directorio de agrupaciones de almacenamiento que se denomina DIR1 en la agrupación de almacenamiento POOL1 para marcarlo como destruido.

```
update stgpooldirectory pool1 dir1 access=destroyed
```

Ejemplo: actualización de un directorio de agrupaciones de almacenamiento para destruirlo en una agrupación de almacenamiento de contenedores en la nube

Actualizar un directorio de agrupación de almacenamiento llamado DIR3 en la agrupación de almacenamiento de contenedor en la nube CLOUDLOCALDISK1 para marcarlo como destruido.

```
update stgpooldirectory cloudlocaldisk1 dir3 access=destroyed
```

Ejemplo: Actualice un directorio de agrupaciones de almacenamiento para que ya no esté disponible

Cuando el directorio de agrupaciones de almacenamiento no está disponible, el servidor no lee datos del directorio ni graba datos en el directorio. Para cambiar la modalidad de acceso a no disponible para un directorio de agrupaciones de almacenamiento, `dir1`, en una agrupación de almacenamiento denominada `pool1`, emita el siguiente mandato:

```
update stgpooldirectory pool1 dir1 access=unavailable
```

Tabla 1. Mandatos relacionados con UPDATE STGPOOLDIRECTORY

Mandato	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.

UPDATE STGRULE (Actualizar una regla de almacenamiento para uno o más agrupaciones de almacenamiento)

Utilice este mandato para actualizar una regla de almacenamiento para una o más agrupaciones de almacenamiento. La regla de almacenamiento planifica niveles entre las agrupaciones de almacenamiento de contenedores. Puede actualizar una o más reglas de almacenamiento para una misma agrupación de almacenamiento de contenedores de destino.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

Sintaxis

```
>>-UPDate STGRULE--nombre_regla----->
>--+-----+----->
| .,-----, |
| v          | |
|'---SRCpools---agrupación_origen+-'
```

```

>+-----+-----+-----+-----+-----+----->
  '-TIERDelay---retardo-' '-MAXProcess---número-'

>+-----+-----+-----+-----+-----+----->
  '-DURation---minutes-+' '-STARTTime---hora-'
    '-NOLimit-'

>+-----+-----+-----+-----+-----+-----<
  '-ACTIVE---No-+' '-DESCRiption---descripción-'
    '-Yes-'

```

Parámetros

nombre_regla(Necesario)

Especifica el nombre de la regla de almacenamiento. La longitud máxima del nombre es de 30 caracteres.

SRCPools

Especifica el nombre de uno o varios directorios de almacenamiento de contenedores de agrupaciones de objetos que se nivelarán a la agrupación de almacenamiento de destino. Para especificar varias agrupaciones de almacenamiento, separe los nombres con comas sin espacios intercalados.

TIERDelay

Especifica el número de días que esperar antes de la regla de almacenamiento nivele los objetos a la siguiente agrupación de almacenamiento. Puede especificar un entero en el rango 0 – 9999. El valor del parámetro se aplica a todos los archivos de la agrupación de almacenamiento.

MAXProcess

Especifica el número máximo de procesos paralelos para completar la regla de almacenamiento para cada agrupación de almacenamiento de origen que se ha especificado. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. Por ejemplo, si tiene 4 agrupaciones de almacenamiento de origen y especifica el valor predeterminado para este parámetro, se inician 32 procesos.

DURation

Especifica el número máximo de minutos que se ejecutará la regla de almacenamiento antes de que se cancele automáticamente. Puede especificar un número comprendido entre 60 y 1440. Si especifica un valor de NOLimit, la regla de almacenamiento se ejecuta hasta que se completa. Este parámetro es opcional.

STARTTime

Especifica el tiempo para el inicio de la ventana en la que la regla de almacenamiento se procesa por primera vez. Este parámetro es opcional. La regla de almacenamiento se ejecuta diariamente dentro de 5 minutos después del tiempo especificado.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	23:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más el número especificado de horas y minutos.	NOW+02:00 o +02:00
NOW-HH:MM o -HH:MM	La hora actual menos el número especificado de horas y minutos.	NOW-02:00 o -02:00

ACTIVE

Especifica si se produce el proceso de la regla de almacenamiento. Este parámetro es opcional. Son posibles los siguientes valores:

No

Especifica que la regla de almacenamiento definida está inactiva. La regla de almacenamiento no se procesa en el momento planificado.

Yes

Especifica que la regla de almacenamiento definida está activa. La regla de almacenamiento se procesa en el momento planificado.

DESCRiption

Especifica una descripción de la regla de almacenamiento. Este parámetro es opcional.

Actualizar una regla de almacenamiento

Actualizar una regla de almacenamiento que se denomina tieraction para mover datos desde las agrupaciones de almacenamiento de contenedores de directorio dirpool1 y dirpool2 a la agrupación de almacenamiento de contenedor en la nube cloudpool1. Especificar una hora de inicio de 23:30:08 horas y un máximo de 16 procesos:

```
update stgrule tieraction srcpools=dirpool1,dirpool2
maxprocess=16 starttime=23:30:08
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE STGRULE

Mandato	Descripción
DEFINE STGRULE	Define una regla de almacenamiento para las agrupaciones de almacenamiento.
DELETE STGRULE	Suprimir reglas de almacenamiento para las agrupaciones de almacenamiento.
QUERY STGRULE	Visualizar información sobre reglas de almacenamiento.

UPDATE VIRTUALFSMAPPING (Actualizar una correlación de espacios de archivos virtuales)

Utilice este mandato para actualizar una definición de correlación de espacio de archivos virtuales.

Restricción: No puede utilizar el mandato UPDATE VIRTUALFSMAPPING para actualizar una correlación de espacio de archivos virtuales para un dispositivo NAS EMC Celerra o EMC VNX. Debe utilizar el mandato DEFINE VIRTUALFSMAPPING.

El dispositivo NAS necesita una definición de desplazador de datos asociados porque cuando el servidor actualiza una correlación de espacio de archivos virtuales, el servidor contacta con el dispositivo NAS para validar el sistema de archivos virtual y el nombre del sistema de archivos.

Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

Sintaxis

```
>>-UPDate VIRTUALFSMapping--nombre_nodo--nombre_espacio_archivos_virtual-->
>--+-----+----->
  '-FILESystem---nuevo_nombre_sistema_archivos-'
>--+-----+-----><
  |                                     .-NAMEType----SERVER-----|
  '-PATH---nuevo_nombre_ruta-----+-----+-----+'
                                     '-NAMEType----+SERVER-----+'
                                     '-HEXadecimal-'
```

Parámetros

nombre_nodo (Necesario)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre_espacio_archivos_virtual (Obligatorio)

Especifica la correlación de espacios de archivos virtuales que se actualizará. No es posible utilizar caracteres comodín ni una lista de nombres.

FILESystem

Especifica el nuevo nombre del sistema de archivos en el que se encuentra la ruta. El nombre del sistema de archivos debe existir en el nodo NAS especificado. El nombre del sistema de archivos no puede contener caracteres comodín. El nombre del

sistema de archivos sólo debería modificarse cuando el nombre del sistema de archivos se ha modificado en el dispositivo NAS o, por ejemplo, cuando se ha trasladado el directorio a un sistema de archivos distinto. Este parámetro es opcional.

PATH

Especifica la nueva ruta desde la raíz del sistema de archivos hasta el directorio. La ruta sólo puede hacer referencia a un directorio. Sólo debería modificarse cuando se ha modificado la ruta del dispositivo NAS o, por ejemplo, cuando se ha trasladado el directorio a una ruta distinta. La longitud máxima de la ruta es de 1024 caracteres. El nombre de ruta es sensible a las mayúsculas y minúsculas. Este parámetro es opcional.

NAMEType

Especifica la forma en la que el servidor debe interpretar el nombre de ruta especificado. Especifique este parámetro sólo si especifica una ruta. Este parámetro es útil cuando una ruta contiene caracteres que no forman parte de la página de códigos en que se ejecuta el servidor. El valor predeterminado es SERVER.

Los valores posibles son:

SERVER

La página de código en la que se está ejecutando el servidor se utiliza para interpretar la ruta.

HEXadecimal

El servidor interpreta el nombre de ruta que ha entrado como la representación hexadecimal de la ruta. Esta opción debe utilizarse cuando una ruta contenga caracteres que no se pueden entrar. Por ejemplo, esto podría ocurrir si el sistema de archivos NAS se establece en un idioma diferente de aquél en que se ejecuta el servidor.

Ejemplo: modificar la ruta de una correlación de espacios de archivos virtuales

Actualizar la correlación de espacios de archivos virtuales /mikeshomedir para el nodo NAS NAS1 modificando la ruta.

```
update virtualfsmapping nas1 /mikeshomedir path=/new/home/mike
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE VIRTUALFSMAPPING

Mandato	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.

UPDATE VOLHISTORY (Actualizar información histórica de volúmenes secuenciales)

Utilice este mandato para actualizar la información histórica de volúmenes de un volumen generado por una copia de seguridad de base de datos o una operación de exportación. Este mandato no se utiliza con los volúmenes de agrupaciones de almacenamiento.

Utilice el mandato UPDATE BACKUPSET para actualizar la información de volúmenes del juego de copias de seguridad en el archivo histórico de volúmenes. No utilice el mandato UPDATE VOLHISTORY para actualizar en el archivo histórico de volúmenes la información de volúmenes correspondiente al juego de copias de seguridad.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento ilimitado.

Sintaxis

```
>>-UPDate VOLHistory--nombre_volumen----->
>--DEVclass----nombre_clase_dispositivo----->
>--+-----+----->
  '-LOcation----ubicación-'
>--+-----+-----><
```

```
'-ORMState-----+MOUNTable-----+'
      +-NOTMOUNTable-----+
      +-COUrier-----+
      +-VAult-----+
      '-COURIERRetrieve-'
```

Parámetros

nombre_volumen (Necesario)

Especifica el nombre del volumen. El volumen debe haberse utilizado para una copia de seguridad de base de datos o una operación de exportación.

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo del volumen.

LOCATION

Especifica la ubicación del volumen. Este parámetro es obligatorio si el parámetro ORMSTATE no se ha especificado. La longitud máxima del texto son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Consejo: El mandato UPDATE VOLHISTORY admite actualizaciones en la información de ubicación y ORMSTATE para los volúmenes de copia de seguridad de instantánea de base de datos.

ORMState

Especifica un cambio en el estado de un volumen de copia de seguridad de base de datos. Este parámetro es necesario si el parámetro LOCATION no se ha especificado. Este parámetro solo se admite en sistemas con licencia de Disaster Recovery Manager. Los estados posibles son:

MOUNTable

El volumen contiene datos válidos y se puede acceder a él para el proceso en el local.

NOTMOUNTable

El volumen está en el local, contiene datos válidos y no se puede acceder a él para proceso en el local.

COUrier

El volumen se está trasladando fuera del local.

VAult

El volumen está fuera del local, contiene datos válidos y no se puede acceder a él para proceso en el local.

COURIERRetrieve

El volumen se está trasladando al local.

Ejemplo: actualizar la ubicación de un volumen que se utiliza para la copia de seguridad de la base de datos

Actualizar la ubicación de un volumen que se utiliza para la copia de seguridad de base de datos, BACKUP1, para mostrar que se ha trasladado a una ubicación fuera del local.

```
update volhistory backup1 devclass=tapebkup
location="700 w. magee rd."
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con UPDATE VOLHISTORY

Mandato	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.

UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

Utilice este mandato para cambiar la modalidad de acceso para uno o varios volúmenes de agrupaciones de almacenamiento.

Una condición de error asociada a un volumen se puede corregir actualizando el volumen a la modalidad de acceso READWRITE. También se puede utilizar este mandato para cambiar la información de ubicación para uno o más volúmenes de agrupaciones de almacenamiento de acceso secuencial.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```

(1)
>>-UPDate Volume-----nombre_volumen----->
>--+-----+----->
  '-ACcEss-----+--READWrite-----+'
      +-READOnly-----+
      +-UNAVailable---+
      |           (2) |
      +-DEStroyed-----+
      |           (3) |
      '-OFFsite-----'
>--+-----+----->
  |           (4) |
  '-LOcAtion-----ubicación-'
.-WHEREStGpool-----*-----
>--+-----+----->
  '-WHEREStGpool-----nombre_agrupación-'
.-WHEREDEVclass-----*-----
>--+-----+----->
  '-WHEREDEVclass-----nombre_clase_dispositivo-'
>--+-----+----->
  |           .-,----- . |
  |           V           | |
  '-WHEREACcEss-----+--READWrite---+--+'
      +-READOnly-----+
      +-UNAVailable--+
      +-OFFsite-----+
      '-DEStroyed---'
>--+-----+----->
  |           .-,----- . |
  |           V           | |
  '-WHEREStAtus-----+--ONline---+--+'
      +-OFFline--+
      +-EMPTy---+
      +-PENding--+
      +-FILLing--+
      '-FULL----'
.-Preview ----No-----
>--+-----+-----><
  '-Preview-----+--No---+'
      '-Yes-'
```

Notas:

1. Debe actualizar como mínimo un atributo (ACCESS o LOCATION).
2. Este valor sólo es válido para los volúmenes de agrupaciones de almacenamiento primarias.
3. Este valor sólo es válido para los volúmenes de agrupaciones de almacenamiento de copia.
4. Este parámetro sólo es válido para los volúmenes de agrupaciones de almacenamiento de acceso secuencial.

Parámetros

nombre_volumen (Necesario)

Especifica el volumen de agrupación de almacenamiento que se actualiza. Puede utilizar caracteres comodín para especificar nombres.

ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor (como, por ejemplo, migración) acceder a los archivos del volumen de agrupación de almacenamiento. Este parámetro es opcional. Los valores posibles son:

READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en el volumen.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en los archivos almacenados en el volumen.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

UNAVailable

Especifica que ni los nodos cliente ni los procesos del servidor pueden acceder a los archivos almacenados en el volumen.

Para que un volumen de acceso aleatorio se convierta en UNAVAILABLE, debe desactivar el volumen. Una vez convertido un volumen de acceso aleatorio en UNAVAILABLE, el volumen no se puede activar.

Si hace que un volumen de acceso secuencial deje de estar disponible, el servidor no intentará montarlo.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

DESTroyed

Especifica que un volumen de agrupación de almacenamiento primaria se ha dañado de modo permanente. Ni los nodos cliente ni los procesos del servidor pueden acceder a los archivos almacenados en el volumen. Utilice esta modalidad de acceso para indicar un volumen completo que debe restaurarse con el mandato RESTORE STGPOOL. Una vez que todos los archivos de un volumen DESTROYED se han restaurado en otros volúmenes, el servidor suprime automáticamente de la base de datos el volumen DESTROYED.

Sólo se pueden actualizar a DESTROYED los volúmenes de agrupaciones de almacenamiento primarias.

Para poder actualizar un volumen de acceso aleatorio al acceso DESTROYED, debe desactivar el volumen. Una vez actualizado el volumen de acceso aleatorio a DESTROYED, no se puede activar el volumen.

Si actualiza un volumen de acceso secuencial a DESTROYED, el servidor no intentará montar el volumen.

Si un volumen no contiene ningún archivo y la modalidad de acceso se cambia a DESTROYED, el servidor suprime el volumen de la base de datos.

Offsite

Especifica que hay un volumen de agrupación de almacenamiento de copia o de datos activos en una ubicación fuera del local desde la que no se puede montar. Sólo pueden tener la modalidad de acceso OFFSITE los volúmenes de las agrupaciones de almacenamiento de copia o de datos activos.

Si especifica valores para ambos parámetros ACCESS y LOCATION, pero la modalidad de acceso no se puede actualizar para un volumen determinado, el atributo de ubicación no se actualiza tampoco para dicho volumen. Por ejemplo, si especifica ACCESS=OFFSITE y el valor LOCATION para un volumen de agrupación de almacenamiento primaria, no se actualizan los valores de acceso ni los de ubicación porque un volumen de agrupación de almacenamiento primaria no puede tener la modalidad de acceso OFFSITE.

LOcation

Especifica la ubicación del volumen. Este parámetro es opcional. Este parámetro únicamente puede especificarse para los volúmenes de agrupaciones de almacenamiento de acceso secuencial. La longitud máxima de la lista de la ubicación es de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco. Para suprimir una ubicación definida anteriormente, especifique una serie nula ("").

WHERESTGpool

Especifica el nombre de la agrupación de almacenamiento para los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización por agrupación de almacenamiento. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de agrupación de almacenamiento, se actualizarán los volúmenes que pertenezcan a cualquier agrupación de almacenamiento.

WHEREDEVclass

Especifica el nombre de la clase de dispositivo de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización por clase de dispositivo. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de clase de dispositivo, se actualizarán los volúmenes que pertenezcan a cualquier clase de dispositivo.

WHEREACcess

Especifica la modalidad de acceso actual de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización a los volúmenes que tienen la modalidad de acceso especificada. Este parámetro es opcional. Puede especificar varias modalidades de acceso separando las modalidades con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la actualización no se restringirá por la modalidad de acceso actual de un volumen. Los valores posibles son:

READWrite

Se actualizan los volúmenes con la modalidad de acceso READWRITE.

READOnly

Se actualizan los volúmenes con la modalidad de acceso READONLY.

UNAVailable

Se actualizan los volúmenes con la modalidad de acceso UNAVAILABLE.

OFFsite

Se actualizan los volúmenes con la modalidad de acceso OFFSITE.

DESTroyed

Se actualizan los volúmenes con la modalidad de acceso DESTROYED.

WHEREStatus

Especifica el estado de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización a los volúmenes que tienen un estado especificado. Este parámetro es opcional. Puede especificar varios valores de estado separando los valores con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la actualización no se restringirá por estado de volumen. Los valores posibles son:

ONline

Se actualizan los volúmenes con el estado ONLINE.

OFFline

Se actualizan los volúmenes con el estado OFFLINE.

EMPTy

Se actualizan los volúmenes con el estado EMPTY.

PENding

Se actualizan los volúmenes con el estado PENDING. Estos son los volúmenes a los que se les han suprimido todos los archivos, pero para los que no ha transcurrido el tiempo especificado mediante el parámetro REUSEDELAY.

FILLing

Se actualizan los volúmenes con el estado FILLING.

FULL

Se actualizan los volúmenes con el estado FULL.

Preview

Especifica si desea previsualizar la operación de actualización sin actualizar realmente los volúmenes. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que los volúmenes se actualizarán.

Yes

Especifica que sólo desea previsualizar la operación de actualización. Esta opción visualiza los volúmenes que se actualizarán, si realiza la operación de actualización.

Ejemplo: establecer que un volumen de cinta no esté disponible

Actualizar un volumen de cinta denominado DSMT20 para que esté no disponible para los nodos cliente y los procesos del servidor.

```
update volume dsmt20 access=unavailable
```

Ejemplo: actualizar la modalidad de acceso de todos los volúmenes fuera del local de una agrupación de almacenamiento específica

Actualizar todos los volúmenes de fuera del local vacíos de la agrupación de almacenamiento TAPEPOOL2. Establecer la modalidad de acceso en READWRITE y suprimir la información de ubicación para los volúmenes actualizados.

```
update volume * access=readwrite location="" wherestgpool=tapepool2  
whereaccess=offsite wherestatus=empty
```





Mandatos relacionados


Tabla 1. Mandatos relacionados con UPDATE VOLUME

Mandato	Descripción
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
VARY	Especifica si está disponible un volumen de disco para el servidor.

Mandatos VALIDATE

Utilice el mandato VALIDATE para verificar que un objeto esté completo o sea válido para IBM Spectrum Protect.

-  Sistemas operativos Linux VALIDATE ASPERA (Validación de una configuración Aspera FASP)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows VALIDATE CLOUD (Validar credenciales de nube)
- VALIDATE LANFREE (Validar rutas fuera de la LAN)
- VALIDATE POLICYSET (Verificar un juego de políticas)
- VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)
- VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

 Sistemas operativos Linux

VALIDATE ASPERA (Validación de una configuración Aspera FASP)

Utilice este mandato para determinar si se puede utilizar la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para optimizar la transferencia de datos en el entorno del sistema. Específicamente, puede determinar si la tecnología Aspera FASP podría resultar en un mejor rendimiento de la red que la tecnología TCP/IP.

Esta mandato verifica los siguientes elementos adicionales:

- Si el entorno del sistema se ha configurado correctamente para utilizar tecnología Aspera FASP
- Si se han instalado las licencias necesarias para habilitar la tecnología Aspera FASP

La tecnología Aspera FASP se utiliza para optimizar la transferencia de datos para la réplica de nodos o para la protección de agrupaciones de almacenamiento en una red de área amplia (WAN). Sin embargo, no es necesario configurar el sistema para que la réplica de nodos o la protección de agrupaciones de almacenamiento ejecuten el mandato VALIDATE ASPERA. Si el sistema se ha configurado para la réplica de nodos o la protección de agrupaciones de almacenamiento en un entorno local, puede emitir el mandato para evaluar si los datos se pueden replicar correctamente en un servidor remoto.

Este mandato solo está disponible en sistemas operativos Linux x86_64.

Antes de emitir el mandato, complete las tareas siguientes:

1. Asegúrese de haber definido al menos un servidor en su entorno del sistema. Emita el mandato PING SERVER para asegurarse de que se puede conectar al servidor definido. Por ejemplo, si el servidor se denomina VMRH6T, emita el mandato siguiente:

```
ping server vmrh6t
```

2. Para utilizar el mandato VALIDATE ASPERA para determinar la velocidad del rendimiento de red, instale licencias de evaluación de 30 días o licencias completas e ilimitadas en los servidores de origen y destino. Por ejemplo, instale licencias en los servidores de origen y destino, VMRH6 y VMRH6T. Para obtener instrucciones sobre cómo obtener e instalar licencias, consulte el apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Para simular un entorno que utiliza varias sesiones, puede ejecutar varias instancias del mandato VALIDATE ASPERA de forma simultánea. Si quiere ejecutar varias sesiones, es posible que quiera limitar el ancho de banda de cada conexión de red para asegurarse de que hay el suficiente ancho de banda disponible para todas las conexiones de red. Para limitar el ancho de banda, especifique la opción de servidor FASPTARGETRATE, tal y como se describe en el apartado FASPTARGETRATE.

Para consultar la cantidad que se está transfiriendo actualmente, emita el mandato QUERY PROCESS:

```
proceso de consulta
```

Puede obtener el número de proceso de la salida del mandato QUERY PROCESS. Puede cancelar el proceso emitiendo el mandato CANCEL PROCESS y especificando el número de proceso, por ejemplo:

```
cancel process 3
```

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-VALidate ASPera--+-----+-----+-----+-----+----->
                        '---nombre_servidor_destino---'

                        .-Wait----No-----.
>--+-----+-----+-----+-----+-----<<
      '-DURation----segundos-'   '-Wait----+No--+-'
                                   '-Yes-'
```

Parámetros

nombre_servidor_destino

Especifica un servidor definido previamente. Este parámetro es opcional. Para especificar este parámetro, siga las directrices:

- Para determinar si Aspera FASP puede optimizar un proceso de réplica de nodo, especifique un servidor de destino que se haya configurado para la réplica de nodos.
- Para determinar si Aspera FASP puede optimizar un proceso de protección de agrupaciones de almacenamiento, especifique un servidor de destino que se haya configurado para la protección de agrupaciones de almacenamiento.
- Para determinar si Aspera FASP puede optimizar la transferencia de datos a un servidor remoto definido, pero no configurado, para la réplica de nodos o la protección de agrupaciones de almacenamiento, especifique ese servidor de destino.
- Si no especifica un servidor de destino, la salida del mandato indica si el servidor de origen se han configurado correctamente para la transmisión de datos de Aspera FASP. La salida indica también si se ha instalado una licencia válida para Aspera FASP en el servidor de origen.

DURation

Especifica el tiempo asignado, en segundos, para transferir datos a través de la red y evaluar el rendimiento. Este parámetro es opcional. El valor predeterminado es de 120 segundos. Puede especificar un valor comprendido entre 120 y 3600000 segundos. El tiempo asignado se divide entre las transferencias de datos Aspera FASP y TCPIP.

Wait

Especifica si se debe esperar a que el servidor termine el proceso de mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los valores siguientes:

No

Especifica que el servidor procesa el mandato en segundo plano. Puede continuar trabajando con otras tareas mientras se procesa el mandato. Si especifica NO, los mensajes de salida se visualizarán en el registro de actividad.

Yes

Especifica que el servidor procesa el mandato en primer plano. La operación debe haber terminado su proceso para poder continuar con otras tareas. Si especifica YES, los mensajes de salida se visualizan en el cliente de línea de mandatos administrativos.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: visualización de información sobre el estado de una configuración de Aspera FASP

En el servidor de origen, ejecute el mandato VALIDATE ASPERA. Para asegurarse de que los mensajes se visualicen en el cliente de línea de mandatos administrativos, especifique WAIT=YES. Consulte el apartado Descripciones de los campos para obtener las

descripciones de los campos.

```
validate aspera wait=yes
```

```
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.  
Amount transferred using FASP: 0 MB per second. Amount transferred using  
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: OK. Days until  
license expires: Never.
```

Ejemplo: verificar si se han instalado las licencias necesarias

En el servidor de origen, ejecute el mandato `VALIDATE ASPERA` y especifique el servidor de réplica de destino. Para asegurarse de que los mensajes se visualicen en el cliente de línea de mandatos administrativos, especifique `WAIT=YES`. Consulte el apartado `Descripciones de los campos` para obtener las descripciones de los campos.

```
validate aspera vmrh6t wait=yes
```

```
ANR0984I Process 8 for VALIDATE ASPERA started in the FOREGROUND at 09:35:21 AM.  
ANR3672E The license file that is required to enable Aspera Fast Adaptive  
Secure Protocol (FASP) technology was not found on the VMRH6 server.  
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.  
Amount transferred using FASP: 0 MB per second. Amount transferred using  
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: Invalid  
configuration. Days until license expires: Expired.  
ANR0985I Process 8 for VALIDATE ASPERA running in the FOREGROUND completed with  
completion state FAILURE at 09:35:21 AM.  
ANR1893E Process 8 for VALIDATE ASPERA completed with a completion state of  
FAILURE.
```

Descripciones de los campos

Estado

Estado de la configuración. Son posibles los siguientes valores:

- `OK` indica que no se han detectado problemas.
- `Invalid configuration` indica que falta un archivo de configuración, archivo de licencia o archivo de biblioteca de Aspera FASP.
- `License issue` indica que hay una licencia que falta, que está caducada o que no es válida.
- `Server failure` indica que se están utilizando todos los puertos, que se ha producido un error de lectura/escritura de red o que no se puede grabar en el archivo de registro de Aspera FASP.
- `Invalid target configuration` indica que falta un archivo de configuración, un archivo de configuración o un archivo de licencia de Aspera FASP en el servidor de destino.
- `Failure on target server` indica que se están utilizando todos los puertos, que se ha producido un error de lectura/escritura de red o que no se puede grabar en el archivo de registro de Aspera FASP.
- `License issue on target server` indica que hay una licencia no válida o caducada en el servidor de destino.
- `Unsupported operating system` indica que se ha instalado un sistema operativo distinto a Linux x86_64 en uno de los servidores o en ambos.
- `Unknown` indica que se ha producido un error inesperado. Para identificar el error, revise los mensajes de registro.

Días que faltan hasta que caduque la licencia

Son posibles los siguientes valores:

- `Never` indica que se ha instalado una licencia completa e ilimitada.
- `Today` indica que se ha instalado una licencia de evaluación de 30 días que caduca hoy.
- `Expired` indica que se ha instalado una licencia de evaluación de 30 días, pero ya ha caducado.
- `Number` indica que se ha instalado una licencia de evaluación de 30 días que caducará dentro del número de días especificado.
- `License not found` indica que no se ha encontrado ninguna licencia.

Cantidad transferida utilizando TCP/IP

La velocidad de la transferencia de datos, en megabytes por segundo, utilizando tecnología TCP/IP.

Cantidad transferida utilizando FASP







Velocidad de la transferencia de datos, en megabytes por segundo, utilizando tecnología Aspera FASP.

Latencia

Latencia de la transferencia de datos en microsegundos.

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE ASPERA

Mandato	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
PING SERVER	Prueba las conexiones entre servidores.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PROTECT STGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Protege una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

VALIDATE CLOUD (Validar credenciales de nube)

Utilice este mandato antes de definir una agrupación de almacenamiento para asegurarse de que las credenciales de una agrupación de almacenamiento de contenedores de nube sean válidas y de que el usuario tenga asignados los permisos necesarios.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
.-CLOUDType--Swift-----
>>-VALIDate CLOud--+----->
      '-CLOUDType--Azure-----'
              +-S3-----+
              +-Softlayer-+
              +-Swift-----+
              '-V1Swift---'

(1)
>--CLOUDUrl-----url_nube--Identity-----identidad_nube----->
>--PAssword-----contraseña----->
>+-----<
  |                               (2) |
  '-BUCKETName-----bucket_name-----'
```

Notas:

1. Si especifica CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY.
2. El parámetro BUCKETNAME es válido sólo si especifica CLOUDTYPE=S3.

Parámetros

CLOUDType

Especifica el tipo de entorno de nube donde está configurando la agrupación de almacenamiento. Puede especificar uno de los siguientes valores:

Azure

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing Microsoft Azure.

S3

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing con el protocolo de servicio de almacenamiento simple (S3), como IBM® Cloud Object Storage o Amazon Web Services (AWS) S3.

Softlayer

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing IBM SoftLayer (IBM Bluemix) con un sistema cloud computing OpenStack Swift.

SWift

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 2 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

V1Swift

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

Este parámetro es opcional. Si no especifica el parámetro, se utiliza el valor predeterminado SWIFT.

CLOUDUrl (Obligatorio)

Especifica la URL del entorno de nube donde se configura la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un punto final de servicio blob, una URL de punto final de región, una dirección IP de accesor, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo `https://` o `http://` al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL se valida cuando empieza la primera copia de seguridad.

IDentity (Obligatorio)

Especifica el ID de usuario para la nube. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si especifica CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

PAssword (Obligatorio)

Especifica la contraseña para la nube. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres.

BUCKETName

Especifica el nombre de un grupo de AWS S3 o una caja fuerte de IBM Cloud Object Storage que se van a utilizar con esta agrupación de almacenamiento, en lugar de utilizar el nombre de grupo o el nombre de caja fuerte predeterminados. Este parámetro es opcional y sólo es válido si especifica CLOUDTYPE=S3. Si existe un grupo o una caja fuerte con el nombre que ha especificado, dicho grupo o dicha caja fuerte se prueba para garantizar que se han establecido los permisos adecuados. Si el grupo o la caja fuerte no existen, el parámetro verifica sólo que el grupo o la caja fuerte con dicho nombre no existan. Siga las restricciones de nombre para el proveedor de nube cuando especifica este parámetro. Revise los permisos del grupo o de la caja fuerte y asegúrese de que las credenciales tengan permiso para leer, escribir, listar y suprimir objetos de este grupo o caja fuerte.

Consejo: Si no especifica el parámetro BUCKETNAME, el ID exclusivo de duplicación global se utilizará como nombre de grupo predeterminado. El valor predeterminado es

```
ibmsp guid
```

donde *guid* es el valor REPLICATION GLOBALLY UNIQUE ID, menos los puntos, en la salida del mandato QUERY REPLSERVER. Por ejemplo, si el ID exclusivo de duplicación global es 52.82.39.20.64.d0.11.e6.9d.77.0a.00.27.00.00.00, el nombre de grupo predeterminado será `ibmsp.5282392064d011e69d770a0027000000`.

Ejemplo: Verificar las credenciales de una agrupación de almacenamiento en el contenedor de nubes S3

Valide las credenciales de la agrupación de almacenamiento en el contenedor de nubes.

```
validate cloud
cloudtype=s3 cloudurl=http://123.234.123.234:5000/v2.0
password=protect8991 bucketname=ibmsp.5282392064d011e69d770a0027000000
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE CLOUD

Mandato	Descripción
DEFINE STGPOOL (contenedor en la nube)	Defina una agrupación de almacenamiento de contenedor en la nube.
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
UPDATE STGPOOL (contenedor de nubes)	Actualizar una agrupación de almacenamiento de contenedores de nube.

VALIDATE LANFREE (Validar rutas fuera de la LAN)

Utilice este mandato para determinar qué destinos de un nodo determinado pueden realizar movimientos de datos sin LAN utilizando un agente de almacenamiento específico.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

```
>>-VALidate LAnfree--nombre_nodo--nombre_agente_alm-----<<
```

Parámetros

nombre_nodo (Obligatorio)

El nombre del nodo que se evaluará.

nombre_stgagent (Obligatorio)

El nombre del agente de almacenamiento que se evaluará.

Ejemplo: validar una configuración fuera de la LAN actual

Validar la configuración y las definiciones de servidor actuales para el nodo TIGER para utilizar el agente de almacenamiento AIX_STA1 para operaciones de datos fuera de la LAN.

```
validate lanfree tiger aix_sta1
```

Nomb. nodo	Agente almacen.	Operación	Nom. clase gestión	Nombre destino	Pos.fuera de LAN?	Explicación	
TIGER	AIX_STA1	COPIA	SEG	STANDARD	OUTPOOL	NO	No hay rutas activas disp.
TIGER	AIX_STA1	COPIA	SEG	STANDARD	PRIMARY	NO	Agrupación almac. destino está configurada para grabación simultánea.
TIGER	AIX_STA1	COPIA	SEG	STANDARD	SHRPOOL	SÍ	
TIGER	AIX_STA1	BACKUP	NOARCH	LFFILE	NO	Agrupación almac. contiene datos deduplicados por clientes y no es accesible para almacenamiento agentes V6.1 o anterior.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	OUTPOOL	NO	No hay rutas activas disp.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	PRIMARY	NO	Agrupación almac. destino está configurada para grabación simultánea.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	SHRPOOL	SÍ		

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE LANFREE

Mandato	Descripción
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY DRIVE	Muestra información sobre las unidades.

Mandato	Descripción
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.

VALIDATE POLICYSET (Verificar un juego de políticas)

Utilice este mandato para verificar que un juego de políticas está completo y es válido antes de activarlo. El mandato examina las definiciones de clase de gestión y de grupo de copia del juego de políticas especificado y notifica las condiciones que debe tener en cuenta antes de activar el juego de políticas.

El mandato VALIDATE POLICYSET no se ejecutará correctamente si se da alguna de las condiciones que se indican a continuación:

- El juego de políticas no tiene ninguna clase de gestión predeterminada.
- Un grupo de copia dentro del juego de políticas especifica una agrupación de almacenamiento de copia como su destino.
- Una clase de gestión especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.
- Se ha especificado un parámetro TOCDESTINATION y la agrupación de almacenamiento es una agrupación de copia o bien tiene un formato de datos distinto de NATIVE o NONBLOCK.

El servidor emite mensajes de aviso para las condiciones siguientes:

- Un grupo de copia especifica una agrupación de almacenamiento que no existe como destino.

Si activa un juego de políticas con grupos de copia que especifican agrupaciones de almacenamiento inexistentes, las operaciones de copia de seguridad o de archivado del cliente no se podrán realizar.

- Una clase de gestión especifica una agrupación de almacenamiento que no existe como destino de los archivos migrados mediante los clientes IBM Spectrum Protect for Space Management.
- El juego de políticas no tiene una o varias de las clases de gestión que existen en el juego de políticas ACTIVE actual.

Si activa el juego de políticas, los archivos de copia de seguridad vinculados con las clases de gestión suprimidas, se volverán a vincular con la clase de gestión predeterminada del nuevo juego de políticas activo.

- El juego de políticas no tiene uno o varios de los grupos de copia que existen en el juego de políticas ACTIVE actual.

Si activa el juego de políticas, dejan de ejecutarse operaciones de copia de seguridad y archivado de los archivos vinculados a las clases de gestión con grupos de copia suprimidos.

- La clase de gestión predeterminada del juego de políticas no contiene un grupo de copia de seguridad o copia archivada.

Si activa el juego de políticas con esta clase de gestión predeterminada, los clientes que utilicen el valor predeterminado no podrán hacer copias de seguridad ni copia archivadas de los archivos.

- Una clase de gestión especifica que debe existir una versión de copia de seguridad para que pueda migrarse un archivo desde un nodo cliente (MIGREQUIRESBKUP=YES), pero la clase de gestión no contiene ningún grupo de copia de seguridad.

Si el servidor tiene la protección de retención de datos activada, deben darse las condiciones siguientes:

- Todas las clases de gestión del juego de políticas que se va a validar deben contener un grupo de copia archivada.
- Si existe una clase de gestión en el juego de políticas activo, debe existir una clase de gestión con el mismo nombre en el juego de políticas que se va a validar.
- Si existe un grupo de copia archivada en el juego de políticas activo, el grupo de copia correspondiente en el juego de políticas que se va a validar debe tener un valor de RETVER que sea por lo menos tan alto como los valores correspondientes en el grupo

de copia activo.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

Sintaxis

```
>>-VALidate Policyset--nombre_dominio--nombre_juego_políticas--<<
```

Parámetros

nombre_dominio (Necesario)

Especifica el nombre del dominio de políticas al que se ha asignado el juego de políticas.

nombre_juego_políticas (Necesario)

Especifica el nombre del juego de políticas que se valida.

Ejemplo: validar un juego de políticas específico

Validar el juego de políticas `VACATION` que se encuentra en el dominio de políticas `EMPLOYEE_RECORDS`.

```
validate policyset employee_records vacation
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE POLICYSET

Mandato	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.

VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)

Utilice esta mandato para identificar las reglas de réplica que se aplican a los espacios de archivos en los nodos de cliente que están configurados para la réplica. También puede utilizar este mandato para verificar que el servidor de réplica de origen puede comunicarse con el servidor de réplica de destino.

Antes de iniciar el proceso de réplica, utilice el mandato `VALIDATE REPLICATION` para determinar si la configuración de réplica es correcta.

Emita este mandato en el servidor que actúe como origen para los datos replicados.

Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

Sintaxis

.,-----.

```

      V                               |
>>-VALIDate REPLication-----nombre_nodo---+----->
      .-VERIFYconnection-----No-----
>--+-----+-----><
      '-VERIFYconnection-----+No--+-'
                               '-Yes-'

```

Parámetros

nombre_nodo (Obligatorio)

Especifica el nombre del nodo de cliente cuyos espacios de archivos desea mostrar. Para especificar varios nombres de nodos de cliente, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

Sólo se muestra información para los nodos de cliente que se han activado o desactivado para la réplica. La modalidad de réplica debe ser SEND. Para determinar si un nodo de cliente está activado o desactivado para la réplica y su modalidad, emita el mandato QUERY NODE. Busque los valores en los campos Estado de réplica y Modalidad de réplica.

VERIFYconnection

Especifica si se debe comprobar la conexión con un servidor de réplica de destino. La versión del servidor de réplica de destino también se comprueba para verificar que sea la versión 6.3 o posterior. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

No se comprueban la conexión y la versión del servidor de réplica de destino.

Sí

Se comprueban la conexión y la versión del servidor de réplica de destino.

Ejemplo: validar la réplica de un nodo de cliente

El nombre del nodo de cliente es NODE1. Verifique el estado de conexión entre los servidores de réplica de origen y destino.

```

validate replication node1 verifyconnection=yes

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: C.S.
Regla de réplica de control: ACTIVE_DATA
      Nivel de regla de réplica: Nivel de sistema
      Nombre de servidor: DRsrv
      Estado de conexión: Conexión válida

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: Arch
Regla de réplica de control: ALL_DATA_HIGH_PRIORITY
      Nivel de regla de réplica: Nivel de nodo
      Nombre de servidor: DRsrv
      Estado de conexión: Conexión válida

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: SpMg
Regla de réplica de control: ALL_DATA
      Nivel de regla de réplica: Nivel de sistema
      Nombre de servidor: DRsrv
      Estado de conexión: Conexión válida

```

Se muestra la salida para todos los tipos de datos, independientemente de si el espacio de archivos contiene los tipos de datos. Por ejemplo, si un espacio de archivos sólo contiene datos de copia de seguridad y archivado, la salida del mandato VALIDATE REPLICATION también contiene información relevante para los datos gestionados por espacio.

Descripciones de los campos

Nombre de nodo

El nodo propietario de los datos replicados.

Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

FSID

El identificador de espacio de archivos del espacio de archivos. El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

Tipo

El tipo de datos. Son posibles los siguientes valores:

Arch

Datos de archivado

C.S.

Datos de copia de seguridad

G.E.

Datos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

Control de norma de réplica

El nombre de la regla de réplica que controla la réplica de un tipo de datos en un espacio de archivos. Para determinar si la regla de control es una regla de espacio de archivos o una regla de servidor, consulte el campo Nivel de regla de réplica.

Nivel de norma de réplica

El nivel de la regla de control en la jerarquía de reglas de réplica. Son posibles los siguientes valores:

Espacio de archivos

La regla de control se asigna a un tipo de datos en el espacio de archivos.

Nodo

La regla de control se asigna a un tipo de datos para un nodo de cliente.

Servidor

La regla de control se asigna a un tipo de datos para todos los espacios de archivos de todos los nodos de cliente que están configurados para la réplica.

Nombre del servidor

El nombre del servidor de réplica de destino que se va a consultar.

Estado de conexión

El estado de conexión entre los servidores de réplica de origen y destino. Son posibles los siguientes valores:

Conexión válida

La comunicación con el servidor de réplica de destino ha sido satisfactoria y el servidor de réplica de destino es un servidor V6.3.

Servidor destino no establecido

El servidor de réplica de destino no se ha establecido. Para establecer el servidor de réplica de destino, emita el mandato SET REPLSERVER.

Anomalía en la comunicación

El servidor de réplica de origen no ha podido ponerse en contacto con el servidor de réplica de destino. Examine el registro de anotaciones de actividad para ver los mensajes de error sobre las comunicaciones anómalas. Las causas posibles son las siguientes:

- La configuración de réplica en el servidor de réplica de origen no es válida. Pueden darse uno o varios de los problemas siguientes:
 - La definición de servidor del servidor de réplica de destino no es correcta.
 - Si la definición del servidor de réplica de destino se ha suprimido y redefinido, emita el mandato PING SERVER para probar la conexión entre el servidor de réplica de origen y destino. Si el mandato PING SERVER es satisfactorio, emita el mandato UPDATE SERVER y especifique FORCESYNC=YES para restablecer las claves de verificación del servidor.

- El nombre del servidor, la dirección de bajo nivel del servidor, la dirección de alto nivel del servidor y la contraseña del servidor no coinciden con los valores que se han especificado en la definición de servidor en el servidor de réplica de destino.
- La configuración de réplica en el servidor de réplica de destino no es válida. Pueden darse uno o varios de los problemas siguientes:
 - La versión del servidor de réplica de destino es anterior a V6.3.
 - La definición de servidor del servidor de réplica de origen no es correcta.
 - El nombre del servidor, la dirección de bajo nivel del servidor, la dirección de alto nivel del servidor y la contraseña del servidor no coinciden con los valores que se han especificado en la definición de servidor en el servidor de réplica de origen.
- Las comunicaciones de red no están disponibles. Para probar la conexión entre el servidor de origen y destino, emita el mandato PING SERVER.
- El servidor de réplica de destino no está disponible.
- Las sesiones entre los servidores de réplica de origen y destino están desactivadas. Para verificar el estado de las sesiones, emita el mandato QUERY STATUS.

Réplica suspendida

El proceso de réplica se suspende cuando restaura la base de datos en el servidor de réplica de origen o inhabilita el proceso de réplica en este servidor emitiendo el mandato DISABLE REPLICATION.

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE REPLICATION

Mandato	Descripción
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del mandato DISABLE o del mandato ACCEPT DATE.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los mandatos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
SET REPLSERVER	Especifica un servidor de réplica de destino.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
UPDATE SERVER	Actualiza la información sobre un servidor.

VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

Utilice este mandato para comparar las políticas para nodos cliente en el servidor de réplica de origen con las mismas políticas en el servidor de réplica de destino donde se replican los datos del nodo cliente.

El mandato muestra las diferencias entre estas políticas para que pueda verificar que las diferencias entre las políticas en los servidores de réplica de origen y destino están pensadas o pueden modificar las políticas en el servidor de réplica de destino.

Asegúrese de que esté instalado IBM Spectrum Protect versión 7.1.1 o posterior en los servidores de réplica de origen y destino antes de emitir este mandato. Emita este mandato en el servidor de réplica de origen.

Clase de privilegio

Cualquier administrador puede emitir este mandato.

Sintaxis

```
>>-VALidate REPLPolicy--+-+-----+-----<<  
                    '-nombre_servidor-'
```

Parámetros

nombre_servidor

Especifica el nombre del servidor de réplica de destino que tiene políticas que desea verificar. Este parámetro es opcional. Si no especifica este parámetro, el mandato establece el servidor de réplica predeterminado como servidor de réplica de destino.

Ejemplo: Visualizar las diferencias entre las políticas de réplica en un servidor de réplica de origen y destino

Para visualizar las diferencias entre las políticas en el servidor de réplica de origen y las políticas en el servidor de réplica de destino, CVTCVS_LXS_SRV2, donde se replican los datos del cliente, emita el mandato siguiente en el servidor de réplica de origen:

```
VALIDATE REPLPOLICY CVTCVS_LXS_SRV2
```

Policy domain name on this server	Policy domain name on target server	Target server name
STANDARD	STANDARD	CVTCVS_LXS_SRV2
Diferencias en conjunto de políticas:		
Change detected	Source server value	Target server value
Mgmt class only on target	Not applicable	STANDARD2
Mgmt Class only on source	STANDARD1	Not applicable
Differences in backup copy group	STANDARD in management class	STANDARD
Change detected	Source server value	Target server value
Versions data exists	2	20

Affected nodes

```
-----  
NODE1,NODE2,NODE3,NODE4,NODE5
```

Descripciones de los campos

Nombre de dominio de políticas en este servidor

Especifica el nombre de dominio de políticas en el servidor de réplica de origen donde se emite el mandato.

Nombre de dominio de políticas en el servidor de destino

Especifica el nombre de dominio de políticas en el servidor de réplica de destino.

Nombre del servidor de destino

Especifica el nombre del servidor de réplica de destino.

Diferencias en conjunto de políticas:

Especifica las diferencias entre las políticas que están definidas en los servidores de réplica de origen y destino. Las diferencias entre las políticas se listan en los campos siguientes:

Cambio detectado

- Valor de servidor de origen
 - Especifica la lista de elementos de políticas que son diferentes entre los servidores de réplica de origen y destino.
- Valor de servidor de destino
 - Especifica el valor para el elemento de la política en el servidor de réplica de origen.
- Valor de servidor de destino
 - Especifica el valor para el elemento de política en el servidor de réplica de destino.

Las diferencias entre el grupo de copia de seguridad <nombre_grupo_copia_seguridad> en la clase de gestión predeterminada O las diferencias en el grupo de copia archivada <nombre_grupo_copia_archivada> en la clase de gestión predeterminada

Especifica las diferencias entre el grupo de copias de seguridad o el grupo de copias archivadas en la clase de gestión. Las diferencias se listan en los campos siguientes:

- Cambio detectado
 - Especifica la lista de campos de grupos de copias que son diferentes.
- Valor de servidor de origen
 - Especifica el valor en el campo de grupo de copia en el servidor de réplica de origen.
- Valor de servidor de destino
 - Especifica el valor en el campo de grupo de copia en el servidor de réplica de destino.

Nodos afectados

Especifica los nombres de todos los nodos cliente que se ven afectados por los cambios que se muestran en esta salida.

Mandatos relacionados

Tabla 1. Mandatos relacionados con VALIDATE REPLPOLICY

Mandato	Descripción
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
SET DISSIMILARPOLICIES	Habilitar las políticas en el servidor de réplica de destino para gestionar los datos replicados.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.

VARY (Activar o desactivar un volumen de acceso aleatorio)

Utilice este mandato para activar o desactivar un volumen de agrupación de almacenamiento de acceso aleatorio en el servidor.

Clase de privilegio

Este mandato sólo es válido para los volúmenes de dispositivos de acceso aleatorio. Este mandato se utiliza, por ejemplo, durante el mantenimiento o durante una acción correctiva de un volumen de acceso aleatorio. No puede activarse un volumen de acceso aleatorio que se haya definido como UNAVAILABLE.

Para emitir este mandato, debe tener privilegio de sistema o privilegio de operador.

Sintaxis

```

>>-VARY---ONline---nombre_volumen---Wait---No-----
      '-Offline-'          '-Wait---No---'
                              '-Yes-'
  
```

Parámetros




- ONline
 - Especifica que el servidor puede utilizar el volumen de acceso aleatorio.
- Offline

Especifica que el servidor no puede utilizar el volumen.
nombre_volumen (Necesario)
 Especifica el identificador del volumen. Los nombres de volumen no pueden contener espacios en blanco intercalados ni signos de igual.





Wait
 Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No
 Especifica que el servidor procesa este mandato como proceso subordinado mientras tiene lugar la ejecución de otras tareas. El servidor visualiza los mensajes que se han creado a partir del proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función del lugar en el que se han anotado los mensajes.



Yes
 Especifica que el servidor procesa este mandato en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida al cliente de administración cuando finaliza el mandato.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows No se puede especificar WAIT=YES desde la consola del servidor.

Ejemplo: activar el volumen

 Sistemas operativos AIX  Sistemas operativos Linux Establecer que el volumen /adsm/stgvol/1 esté disponible para que el servidor pueda utilizarlo como volumen de agrupación de almacenamiento.  Sistemas operativos AIX  Sistemas operativos Linux

```
vary online /adsm/stgvol/1
```

 Sistemas operativos Windows Establecer que el volumen j:\storage\pool001 esté disponible para que el servidor pueda utilizarlo como volumen de agrupación de almacenamiento.  Sistemas operativos Windows

```
vary online j:\storage\pool001
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con VARY

Mandato	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.

Opciones de servidor

Durante la instalación, IBM Spectrum Protect proporciona un archivo de opciones de servidor que contiene un conjunto de opciones predeterminadas para iniciar el servidor.

El archivo es:

- dmserv.opt en el directorio de instancia de servidor

Las opciones de servidor permiten personalizar lo siguiente:


- Comunicaciones
- Almacenamiento de servidor
- Cliente-servidor
- Fecha, número, hora e idioma
- Anotaciones de recuperación y base de datos
- Transferencia de datos
- Mensaje


- Anotaciones de eventos
- Seguridad y sistema de licencias







Varias opciones que pueden utilizarse para diversas finalidades. Estas opciones no documentadas están pensadas para que las utilice solo el soporte de IBM®.


Para visualizar los valores actuales de las opciones, escriba:






```
query option
```











- **Modificación de opciones del servidor**
El servidor lee el archivo de opciones del servidor durante la inicialización del servidor. Cuando actualiza una opción del servidor editando el archivo, debe detener y arrancar el servidor para activar el archivo de opciones del servidor actualizado.
- **Tipos de opciones del servidor**
Las opciones del servidor le permiten personalizar el modo en que funcionan algunas funciones y procesos.
- **3494SHARED**
La opción 3494SHARED especifica si una biblioteca IBM 3494 puede compartir aplicaciones distintas de IBM Spectrum Protect.
- **ACSACCESSID**
La opción ACSACCESSID especifica el identificador del control de acceso de ACS para una biblioteca ACSLS.
- **ACSLOCKDRIVE**
La opción ACSLOCKDRIVE especifica si las unidades de las bibliotecas ACSLS están bloqueadas. Al bloquear las unidades, se garantiza el uso exclusivo de la unidad de la biblioteca ACSLS en un entorno compartido. Sin embargo, el rendimiento es mejor si las bibliotecas no se bloquean. Cuando otras aplicaciones no comparten las unidades de IBM Spectrum Protect, no es necesario bloquear las unidades.
- **ACSQUICKINIT**
La opción ACSQUICKINIT especifica si, en el arranque del servidor, la inicialización de la biblioteca ACSLS es rápida o completa. El valor predeterminado es Yes. Una inicialización rápida evita la sobrecarga asociada con la sincronización del inventario del servidor de IBM Spectrum Protect con el inventario de biblioteca ACSLS (mediante una auditoría de la biblioteca).
- **ACSTIMEOUTX**
La opción ACSTIMEOUTX especifica el múltiplo del valor de tiempo de espera incorporado de las API ACSLS. El valor de tiempo de espera incorporado de la API de introducción, expulsión y auditoría ACS son 1800 segundos; el valor de todas las demás API ACSLS son 600 segundos. Por ejemplo, si el múltiplo especificado es 5, el valor de tiempo de espera de la API de auditoría serán 9000 segundos y el valor de todas las demás API serán 3000 segundos.
- **ACTIVELOGDIRECTORY**
La opción ACTIVELOGDIRECTORY especifica el nombre del directorio donde están almacenados todos los registros activos.
- **ACTIVELOGSIZE**
La opción ACTIVELOGSIZE establece el tamaño total del registro.
- **ADMINCOMMTIMEOUT**
La opción ADMINCOMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos.
- **ADMINIDLETIMEOUT**
La opción ADMINIDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente administrativo puede estar desocupada antes de que la cancele el servidor.
- **ADMINONCLIENTPORT**
La opción ADMINONCLIENTPORT especifica si las sesiones administrativas pueden utilizar TCPPOINT. El valor predeterminado es YES.
-  **Sistemas operativos WindowsADSMGROUPNAME**
La opción ADSMGROUPNAME especifica el nombre de un grupo Windows. Un nodo cliente debe ser miembro de este grupo para poder utilizar el servidor de IBM Spectrum Protect a través de NT Unified Logon. El nodo de cliente también debe ser un nodo de cliente de IBM Spectrum Protect registrado.
- **ALIASHALT**
La opción ALIASHALT permite a los administradores asignar un nombre diferente a un mandato **HALT** de IBM Spectrum Protect.
- **ALLOWDESAUTH**
La opción ALLOWDESAUTH especifica si se debe permitir la utilización del algoritmo DES (Data Encryption Standard) para la autenticación entre un servidor y un cliente de archivado y copia de seguridad.
- **ALLOWREORGINDEX**
La opción ALLOWREORGINDEX especifica si la reorganización de índice iniciada por el servidor está activada o desactivada.
- **ALLOWREORGTABLE**
La opción ALLOWREORGTABLE especifica si la reorganización de tabla iniciada por el servidor está activada o desactivada.
- **ARCHFAILOVERLOGDIRECTORY**
La opción ARCHFAILOVERLOGDIRECTORY especifica el directorio que utiliza el servidor para almacenar los archivos de registro de archivado que no se pueden almacenar en el directorio de registros de archivado.
- **ARCHLOGCOMPRESS**
Puede habilitar o inhabilitar la compresión de registros de archivado en el servidor de IBM Spectrum Protect. Al comprimir los registros de archivado, se reduce la cantidad de espacio necesaria para el almacenamiento.




- **ARCHLOGDIRECTORY**
La opción ARCHLOGDIRECTORY especifica un directorio en el que el gestor de base de datos puede archivar un archivo de registro una vez completadas todas las transacciones representadas en dicho archivo de registro.
- **ARCHLOGUSEDTHRESHOLD**
La opción ARCHLOGUSEDTHRESHOLD especifica cuándo iniciar una copia de seguridad de base de datos automática en relación con el porcentaje de espacio de archivo de anotaciones de archivado utilizado. El valor predeterminado es el 80 por ciento.
- **ASSISTVCRRECOVERY**
La opción ASSISTVCRRECOVERY especifica si IBM Spectrum Protect debe ayudar a una unidad IBM 3590 a recuperarse de una condición de VCR (Vital Cartridge Records) perdidos o dañados. Si especifica YES (el valor predeterminado) y si IBM Spectrum Protect detecta un error durante el proceso de montaje, se sitúa al final de los datos durante el proceso de desmontaje para permitir que las unidades restauren el VCR. Durante la operación de cinta, es posible que se produzca un pequeño efecto sobre el rendimiento ya que la unidad no puede realizar una búsqueda rápida con un VCR perdido o dañado. Sin embargo, no se produce ninguna pérdida de datos.
- **AUDITSTORAGE**
Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento del servidor utilizado para operaciones de copia de seguridad y archivado, y para archivos bajo gestión de espacio. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de CPU y puede detener otras actividades del servidor. Puede utilizar la opción AUDITSTORAGE para especificar que el almacenamiento no se ha de calcular como parte de una auditoría de licencias.
- **BACKUPINITIATIONROOT**
La opción BACKUPINITIATIONROOT especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.
- **CHECKTAPEPOS**
La opción CHECKTAPEPOS especifica si el servidor de IBM Spectrum Protect valida la posición de los bloques de datos en la cinta.
- **CLIENTDEDUPTXNLIMIT**
La opción CLIENTDEDUPTXNLIMIT especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.
- **CLIENTDEPLOYCATALOGURL**
La opción CLIENTDEPLOYCATALOGURL especifica la ubicación del archivo de catálogo que se utiliza para las operaciones de despliegue de cliente automático.
- **CLIENTDEPLOYUSELOCALCATALOG**
La opción CLIENTDEPLOYCATALOGURL especifica si la versión local del archivo de catálogo se utiliza para las operaciones de despliegue de cliente automático.
- **COMMMETHOD**
La opción COMMMETHOD especifica el método de comunicaciones que utilizará el servidor.
- **COMMTIMEOUT**
La opción COMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente durante una operación que produce una actualización de la base de datos. Si el tiempo supera este tiempo de espera, el servidor finaliza la sesión con el cliente. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera. Los clientes pueden exceder el tiempo de espera si existe una gran carga de red en el entorno o realizan copias de seguridad de archivos grandes.
- **CONTAINERRESOURCESTIMEOUT**
La opción CONTAINERRESOURCESTIMEOUT especifica durante cuánto tiempo espera el servidor a completar una operación de almacén de datos en una agrupación de almacenamiento de contenedor.
-  **Sistemas operativos Windows DATEFORMAT**
La opción DATEFORMAT especifica el formato que el servidor ha de utilizar para visualizar las fechas.
- **DBDIAGLOGSIZE**
Esta opción permite controlar el espacio que utilizan los archivos de registro de diagnóstico.
- **DBDIAGPATHFSTHRESHOLD**
La opción DBDIAGPATHFSTHRESHOLD especifica un umbral para el espacio libre en el sistema de archivos o disco que contiene el archivo db2diag.log .
- **DBMEMPERCENT**
Utilice esta opción para especificar el porcentaje de memoria del espacio de direcciones virtuales dedicado a procesos del gestor de bases de datos.
- **DBMTCPPORT**
La opción DBMTCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del gestor de base de datos espera las peticiones de sesiones de cliente.
- **DEDUPREQUIRESBACKUP**
La opción DEDUPREQUIRESBACKUP especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la deduplicación de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.
- **DEDUPTIER2FILESIZE**
La opción DEDUPTIER2FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación

- de datos duplicados de nivel 2.
- DEDUPTIER3FILESIZE
La opción DEDUPTIER3FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 3.
- DEVCONFIG
La opción DEVCONFIG especifica el nombre de un archivo en el que el usuario quiere que IBM Spectrum Protect almacene una copia de seguridad de la información de configuración del dispositivo.
- DISABLEREORGTABLE
La opción DISABLEREORGTABLE especifica si está inhabilitada la reorganización de tabla para los nombres de tabla especificado en la lista de tablas.
- DISABLESCHEDULES
La opción DISABLESCHEDULES especifica si se desactivan las planificaciones de cliente y de administración durante una recuperación del servidor de IBM Spectrum Protect.
- DISPLAYLFINFO
La opción DISPLAYLFINFO especifica el modo en que los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del nodo.
- DNSLOOKUP
La opción DNSLOOKUP especifica si el servidor utiliza llamadas de API del sistema para determinar los nombres de servidor de nombres de dominio (DNS) de los sistemas que establecen contacto con el servidor.
- DRIVEACQUIRERETRY
La opción DRIVEACQUIRERETRY le permite especificar el número de veces que el servidor reintentará la adquisición de una unidad en una biblioteca IBM 349x. Si se comparte la biblioteca entre varias aplicaciones, puede parecer que sus unidades están disponibles en el servidor (mediante un proceso subordinado de sondeo), cuando en realidad no lo están.
- ENABLENASDEDUP
La opción de servidor ENABLENASDEDUP especifica si el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos de almacenamiento conectado a red (NAS). Esta opción solo se aplica a los servidores de archivos NetApp.
- EVENTSERVER
La opción EVENTSERVER especifica si, en el momento del arranque, el servidor debe intentar establecer contacto con el servidor de eventos.
- EXPINTERVAL
La opción EXPINTERVAL especifica el intervalo, en horas, que ha de transcurrir entre los procesos automáticos de caducidad de inventario que realiza IBM Spectrum Protect. El proceso de caducidad de inventario elimina las copias de seguridad y las copias archivadas del servidor, según se haya especificado mediante las clases de gestión a las que están vinculados los archivos del cliente. Si no se ejecuta periódicamente el proceso de caducidad, no se reclamará el espacio de agrupación de almacenamiento de los archivos del cliente caducados, y el servidor necesitará más espacio de almacenamiento del que necesita según la política.
- EXPQUIET
La opción EXPQUIET especifica si IBM Spectrum Protect ha de enviar mensajes detallados durante el proceso de caducidad.
-  Sistemas operativos Linux  Sistemas operativos Windows FASPBEGPORT
La opción FASPBEGPORT especifica el número inicial en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).
-  Sistemas operativos Linux  Sistemas operativos Windows FASPENDPORT
La opción FASPENDPORT especifica el número final en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).
-  Sistemas operativos Linux  Sistemas operativos Windows FASPTARGETRATE
La opción FASPTARGETRATE especifica la tasa de destino para la transferencia de datos con la tecnología Aspera Fast Adaptive Secure Protocol (FASP). Si especifica la tasa de destino, limita el ancho de banda de cada conexión de red que utiliza la tecnología Aspera FASP. De este modo, puede asegurarse de que hay suficiente ancho de banda disponible para todas las conexiones de red.
- FFDCLOGLEVEL
La opción FFDCLOGLEVEL especifica el tipo de mensajes del servidor generales que se muestran en el registro FFDC (First Failure Data Capture).
- FFDCLOGNAME
La opción FFDCLOGNAME especifica un nombre del registro FFDC (First Failure Data Capture).
- FFDCMAXLOGSIZE
La opción FFDCMAXLOGSIZE especifica el tamaño del archivo de registro FFDC (First Failure Data Capture).
- FFDCNUMLOGS
La opción FFDCNUMLOGS especifica el número de archivos de registro que se pueden utilizar para el registro circular. El valor predeterminado es 10.
- FILEEXIT
La opción FILEEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es un registro del archivo.
- FILETEXTEXIT
La opción FILETEXTEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado

- cronológicamente es una línea con un tamaño fijo que puede leerse.
- **FSUSEDTHRESHOLD**
La opción FSUSEDTHRESHOLD especifica qué porcentaje del sistema de archivos puede llenar la base de datos antes emitir un mensaje de alerta.
 - **IDLETIMEOUT**
La opción IDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente puede estar desocupada antes de que la cancele el servidor. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera si existe una gran carga en la red del entorno. Observe, sin embargo, que una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.
 - **KEEPALIVE**
La opción KEEPALIVE especifica si la función keepalive del protocolo de control de transmisiones (TCP) está habilitada para los sockets TCP de salida. La función keepalive TCP envía una transmisión de un dispositivo a otro para comprobar que el enlace entre los dos dispositivos está operativo.
 - **KEEPALIVETIME**
La opción KEEPALIVETIME especifica la frecuencia con la que TCP envía una transmisión de estado activo cuando recibe una respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.
 - **KEEPALIVEINTERVAL**
La opción KEEPALIVEINTERVAL especifica la frecuencia con la que se envía una transmisión de estado activo, si no se recibe ninguna respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.
 - **LANGUAGE**
La opción LANGUAGE controla la inicialización de los entornos nacionales. Un entorno nacional incluye el idioma y los formatos de fecha, hora y número que se han de utilizar para la consola y el servidor.
 - **LDAPCACHEDURATION**
La opción LDAPCACHEDURATION determina la cantidad de tiempo que el servidor IBM Spectrum Protect almacena en memoria caché la información de autenticación de contraseña LDAP.
 - **LDAPURL**
La opción LDAPURL especifica la ubicación de un servidor LDAP (Lightweight Directory Access Protocol). Establezca la opción de LDAPURL después de configurar el servidor LDAP.
 - **MAXSESSIONS**
La opción MAXSESSIONS especifica el número máximo de sesiones cliente simultáneas que se pueden conectar con el servidor.
 - **MESSAGEFORMAT**
La opción MESSAGEFORMAT especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.
 - **MIRRORLOGDIRECTORY**
La opción MIRRORLOGDIRECTORY especifica el directorio para duplicar la vía de acceso de registro activo.
 - **MOVEBATCHSIZE**
La opción MOVEBATCHSIZE especifica el número de archivos cliente que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Este movimiento de datos es el resultado de las operaciones de restauración y copia de seguridad de agrupaciones de almacenamiento, de migración, reclamación y MOVE DATA. Esta opción funciona con la opción MOVESIZETHRESH.
 - **MOVESIZETHRESH**
La opción MOVESIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Cuando se alcance este umbral, no se agregarán más archivos al lote actual, y se arrancará una nueva transacción después de que se haya trasladado el lote actual.
 - **MSGINTERVAL**
La opción MSGINTERVAL especifica el tiempo, en minutos, entre los mensajes que solicitan a un operador que monte una cinta para el servidor.
 -  **Sistemas operativos Windows NAMEDPIPENAME**
La opción NAMEDPIPENAME especifica un método de comunicaciones que permite que los procesos se comuniquen entre sí sin tener que saber dónde los procesos del emisor y remitente están ubicados. El nombre actúa como un alias, y conecta los dos procesos independientemente de si están en el mismo sistema o en otros dominios conectados.
 - **NDMPCONNECTIONTIMEOUT**
La opción de servidor NDMPCONNECTIONTIMEOUT especifica el tiempo, en horas, que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante las operaciones de restauración NDMP a través de la LAN. Las operaciones de restauración NDMP de sistemas de archivos NAS de gran tamaño puede tener periodos prolongados de inactividad. El valor predeterminado es 6.
 - **NDMPCONTROLPORT**
La opción NDMPCONTROLPORT especifica el número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP (Network Data Management Protocol). El servidor de IBM Spectrum Protect no funciona como un servidor de cintas NDMP de uso general.
 - **NDMPENABLEKEEPALIVE**
La opción del servidor NDMPENABLEKEEPALIVE especifica si el servidor de IBM Spectrum Protect habilita el mantenimiento en actividad de TCP (Transmission Control Protocol) en las conexiones control NDMP (network data-management protocol) en dispositivos NAS (network-attached storage). El valor predeterminado es NO.

- 
Sistemas operativos AIX **Sistemas operativos Linux** **Sistemas operativos Windows****NDMPKEEPIDLEMINUTES**
 La opción de servidor NDMPKEEPIDLEMINUTES especifica la cantidad de tiempo, en minutos, antes de que el sistema operativo transmita el primer paquete de estado activo TCP (Transmission Control Protocol) en una conexión de control NDMP (Network Data-Management Protocol). El valor predeterminado son 120 minutos.
- NDMPPORTRANGE**
 La opción NDMPPORTRANGE especifica el rango de números de puerto por los que IBM Spectrum Protect pasa en secuencia para obtener un número de puerto para aceptar una sesión de un dispositivo NAS (almacenamiento conectado a red) para la transferencia de datos. El valor predeterminado es 0,0, que significa que IBM Spectrum Protect deja que el sistema operativo proporcione un puerto (puerto efímero).
- NDMPPREFDATAINTERFACE**
 Esta opción especifica la dirección IP que se asocia a la interfaz en la que desea que el servidor reciba todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
- NOPREEMPT**
 El servidor permite que determinadas operaciones tengan prioridad sobre otras operaciones para acceder a volúmenes y dispositivos. Puede especificar la opción NOPREEMPT para desactivar la prioridad. Cuando se desactiva la prioridad, ninguna operación puede tener prioridad sobre otra para acceder a un volumen, y únicamente una operación de copia de seguridad de base de datos puede tener prioridad sobre otra operación para acceder a un dispositivo.
- NORETRIEVEDATE**
 La opción NORETRIEVEDATE especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo. Esta opción y el parámetro MIGDELAY de agrupación de almacenamiento controlan cuándo el servidor migra los archivos.
- 
Sistemas operativos Windows**NPAUDITFAILURE**
 La opción NPAUDITFAILURE especifica si ha de enviarse un evento a las anotaciones de eventos cuando un nodo se conecte con el servidor utilizando un nombre que se encuentra en el grupo de Windows pero que no coincide con el nombre de inicio de sesión de cuenta de Windows. Para garantizar que un nodo pueda acceder sólo a sus propios datos, el nombre del nodo y el nombre de cuenta Windows deben coincidir.
- 
Sistemas operativos Windows**NPAUDITSUCCESS**
 La opción NPAUDITSUCCESS especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.
- 
Sistemas operativos Windows**NPBUFFERSIZE**
 La opción NPBUFFERSIZE especifica el tamaño del búfer de comunicaciones de Named Pipes.
- 
Sistemas operativos Windows**NUMBERFORMAT**
 La opción NUMBERFORMAT especifica el formato de numeración que el servidor utiliza para visualizar los números.
- NUMOPENVOLSALLOWED**
 La opción NUMOPENVOLSALLOWED especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.
- PUSHSTATUS**
 La opción PUSHSTATUS se utiliza en servidores de radio para asegurarse de que la información de estado se envía al servidor concentrador. No actualice esta opción a menos que deba restaurar la configuración del Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o de radio.
- QUERYAUTH**
 La opción QUERYAUTH especifica el nivel de autorización de administración necesario para emitir los mandatos QUERY o SQL SELECT. De forma predeterminada, cualquier administrador puede emitir los mandatos QUERY y SELECT. Puede utilizar esta opción para restringir el uso de estos mandatos.
- RECLAIMDELAY**
 Esta opción retrasa la reclamación de un volumen SnapLock y permite que los datos restantes caduquen para que no haya necesidad de reclamar el volumen.
- RECLAIMPERIOD**
 Esta opción permite definir el número de días para el periodo de reclamación de un volumen SnapLock.
- REORGBEGINTIME**
 La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o índice.
- REORGDURATION**
 La opción REORGDURATION especifica un intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.
- REPORTRETRIEVE**
 La opción REPORTRETRIEVE genera informes sobre las operaciones de restauración o recuperación que realizan los nodos clientes o los administradores. El valor predeterminado es NO.
- REPLBATCHSIZE**
 La opción REPLBATCHSIZE especifica el número de archivos de cliente que se van a replicar en proceso por lotes, dentro de la misma transacción de servidor. Esta opción afecta únicamente a los procesos de réplica de nodo y funciona con la opción REPLSIZETHRESH para mejorar el proceso de réplica de nodo.
- REPLSIZETHRESH**
 La opción REPLSIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos replicados, dentro de la misma

- transacción del servidor.
- **REQSYSAUTHOUTFILE**
La opción REQSYSAUTHOUTFILE especifica si es necesaria la autorización del sistema para los mandatos de administración que hacen que IBM Spectrum Protect realice una grabación en un archivo externo.
 - **RESOURCETIMEOUT**
La opción RESOURCETIMEOUT especifica el intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso. Cuando se exceda el tiempo de espera, la petición del recurso se cancelará.
 - **RESTHTTPSPORT**
La opción RESTHTTPSPORT especifica el número de puerto que se utilizará para la comunicación mediante el Protocolo seguro de transferencia de hipertexto (HTTPS) entre el Centro de operaciones y el servidor concentrador.
 - **RESTOREINTERVAL**
La opción RESTOREINTERVAL especifica durante cuánto tiempo se puede guardar una sesión de restauración rearrancable en la base de datos del servidor. Siempre y cuando la sesión de restauración se haya guardado en la base de datos, se puede volver a arrancar desde el punto en el que se ha detenido.
 - **RETENTIONEXTENSION**
La opción RETENTIONEXTENSION especifica el número de días que ha de ampliarse la fecha de retención de un volumen de SnapLock. Esta opción permite que el servidor amplíe la fecha de retención de un volumen de SnapLock para evitar las reclamaciones excesivas.
 -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANDISCOVERY**
La opción SANDISCOVERY especifica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.
 -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANDISCOVERYTIMEOUT**
La opción SANDISCOVERYTIMEOUT especifica la cantidad de tiempo permitido para que respondan los adaptadores de bus de host si se consulta mediante el proceso de descubrimiento de SAN. Cuando se alcance el tiempo especificado en SANDISCOVERYTIMEOUT, el proceso excede el tiempo de espera.
 -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANREFRESHTIME**
La opción SANREFRESHTIME especifica la cantidad de tiempo que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. La opción SANREFRESHTIME tiene un valor predeterminado de 0, que significa que no hay caché de descubrimiento de SAN. La información se obtiene directamente del adaptador de bus de host (HBA) cada vez que el servidor ejecuta una operación de descubrimiento de SAN.
 - **SEARCHMPQUEUE**
La opción SEARCHMPQUEUE especifica el orden en el que el servidor da respuesta a las peticiones de la cola de montaje. Si se especifica la opción, el servidor primero intenta satisfacer las peticiones de los volúmenes que ya están montados. Estas peticiones pueden ser satisfechas antes que otras peticiones, aunque estas otras hayan estado esperando más tiempo el punto de montaje. Si no se especifica esta opción, el servidor satisface las peticiones en el orden en que éstas se reciben.
 -  Sistemas operativos Windows **SECUREPIPES**
Cuando se utiliza el protocolo Named Pipes, si se activa SECUREPIPES, el servidor se ve forzado a comprobar el grupo Windows designado por ADMSGROUPNAME a fin de autenticar un nodo/usuario cliente.
 - **SERVERDEDUPTXNLIMIT**
La opción SERVERDEDUPTXNLIMIT especifica el tamaño máximo de los objetos que pueden tener optimización de almacenamiento en el servidor.
 - **SHMPORT**
 Sistemas operativos AIX  Sistemas operativos Linux La opción SHMPORT especifica la dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Todas las comunicaciones de memoria compartida comienzan por una conexión TCP/IP.  Sistemas operativos Windows La opción SHMPORT especifica el puerto en el que el servidor está a la escucha de conexiones de memoria compartida.
 - **SHREDDING**
La opción SHREDDING especifica si la destrucción de datos confidenciales suprimidos se lleva a cabo automática o manualmente. La destrucción sólo se aplica a los datos de las agrupaciones de almacenamiento que se han configurado explícitamente para dar soporte a la destrucción.
 - **SNMPHEARTBEATINTERVAL**
La opción SNMPHEARTBEATINTERVAL especifica el intervalo en minutos entre consultas del servidor de IBM Spectrum Protect.
 - **SNMPMESSAGECATEGORY**
La opción SNMPMESSAGECATEGORY especifica los tipos de detecciones que se utilizan cuando se envían los mensajes desde el servidor, a través del subagente SNMP (Simple Network Management Protocol), al gestor SNMP.
 - **SNMPSUBAGENT**
La opción SNMPSUBAGENT especifica los parámetros necesarios para que el subagente de IBM Spectrum Protect se comunique con el daemon SNMP (Simple Network Management Protocol). Esta opción únicamente sirve para configurar el subagente SNMP para las comunicaciones con el agente SNMP; el servidor la ignora.
 - **SNMPSUBAGENTHOST**
La opción SNMPSUBAGENTHOST especifica la ubicación del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect. El valor predeterminado para esta opción es 127.0.0.1.
 - **SNMPSUBAGENTPORT**
La opción SNMPSUBAGENTPORT especifica el número de puerto del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect.

- **SSLFIPSMODE**
La opción SSLFIPSMODE especifica si se aplica la modalidad Estándar federal de procesamiento de información (FIPS) para la capa de sockets seguros (SSL). El valor predeterminado es NO.
- **SSLINITTIMEOUT**
La opción SSLINITTIMEOUT especifica el tiempo, en minutos, que el servidor espera a que finalice la inicialización de una sesión SSL (capa de sockets seguros) antes de que cancelar la sesión.
- **SSLTCPADMINPORT**
La opción SSLTCPADMINPORT especifica la dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera peticiones solo de sesiones con SSL habilitado. Las sesiones son para el cliente de administración de línea de mandatos.
- **SSLTCPSPORT**
La opción SSLTCPSPORT especifica el número de puerto de capa de sockets seguros (SSL) solo para las sesiones compatibles con SSL. La unidad de comunicación TCP/IP del servidor espera peticiones en este puerto para sesiones con SSL activada del cliente.
- **TCPADMINPORT**
La opción TCPADMINPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las peticiones de sesiones compatibles con TCP/IP y SSL distintas de las sesiones de cliente. Esto incluye las sesiones de administración, las sesiones de servidor a servidor, las sesiones del agente de almacenamiento, las sesiones del cliente de biblioteca, las sesiones de servidor gestionado y las sesiones del servidor de eventos.
-  Sistemas operativos AIX  Sistemas operativos Linux **TCPBUFSIZE**
La opción TCPBUFSIZE especifica el tamaño del búfer utilizado para peticiones de envío TCP/IP. Durante una restauración, los datos de cliente se traspasan del componente de sesión IBM Spectrum Protect a un controlador de comunicaciones TCP. La opción TCPBUFSIZE determina si el servidor envía los datos directamente desde el búfer de la sesión o copia los datos en el búfer TCP. Un tamaño de búfer de 32 KB dará lugar a que servidor copie forzosamente los datos en su búfer de comunicaciones y al vaciado del búfer cuando éste esté lleno.
- **TCPNODELAY**
La opción TCPNODELAY especifica si el servidor inhabilita el retraso al enviar pequeños paquetes sucesivos en la red.
- **TCPSPORT**
La opción TCPSPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. El controlador de comunicación TCP/IP de servidor escucha este puerto tanto para las sesiones TCP/IP como para las sesiones compatibles con SSL desde el cliente.
- **TCPWINDOWSIZE**
La opción TCPWINDOWSIZE especifica, en kilobytes, la cantidad de datos de recepción que se pueden almacenar en el búfer a la vez en una conexión TCP/IP. El host emisor no puede enviar más datos hasta que reciba una confirmación y una actualización de ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP anunciada en la conexión. Una ventana más grande permite que el emisor continúe enviando datos y puede mejorar el rendimiento de las comunicaciones, sobre todo en las redes rápidas con una latencia elevada.
- **TECBEGINEVENTLOGGING**
La opción TECBEGINEVENTLOGGING especifica si las anotaciones de eventos del receptor de TIVOLI deben empezar cuando se inicie el servidor. Si se especifica la opción TECHOST, TECBEGINEVENTLOGGING toma de forma predeterminada el valor YES.
- **TECHOST**
La opción TECHOST especifica el nombre de host o dirección IP del servidor de eventos de Tivoli.
- **TECPORT**
La opción TECPORT especifica la dirección de puerto TCP/IP en la que el servidor de eventos Tivoli está a la escucha. Esta opción sólo es necesaria si el servidor de eventos Tivoli se encuentra en un sistema que no tiene un servicio PortMapper en funcionamiento.
- **TECUTF8EVENT**
La opción TECUTF8EVENT permite al administrador de IBM Spectrum Protect enviar información al servidor de Tivoli Enterprise Console (TEC) en formato de datos UTF-8. El valor predeterminado es No. Puede visualizar si esta opción está activada o no mediante la emisión del mandato QUERY OPTION.
- **THROUGHPUTDATATHRESHOLD**
La opción THROUGHPUTDATATHRESHOLD especifica un umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele después de que se haya alcanzado el umbral de tiempo.
- **THROUGHPUTTIMETHRESHOLD**
La opción THROUGHPUTTIMETHRESHOLD especifica el umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.
-  Sistemas operativos Windows **TIMEFORMAT**
La opción TIMEFORMAT especifica el formato mediante el cual el servidor visualiza la hora.
- **TXNGROUPMAX**
La opción TXNGROUPMAX especifica el número de objetos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones. El valor mínimo es de 4 objetos y el valor máximo es de 65000 objetos. El valor predeterminado son 4096 objetos. Los objetos transferidos son directorios, archivos reales o ambos. El servidor cuenta cada archivo o directorio como un objeto.
- **UNIQUETDPTEEVENTS**
La opción UNIQUETDPTEEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje

individual de IBM Spectrum Protect, incluidos los mensajes del cliente, del servidor y del cliente de IBM Spectrum Protect. El valor predeterminado es No.

- UNIQETECEVENTS

La opción UNIQETECEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect. El valor predeterminado es No.

- USEREXIT

La opción USEREXIT especifica la salida definida por el usuario a la que se otorgará control para poder gestionar un evento.

- VERBCHECK

La opción VERBCHECK especifica que el servidor realizará una comprobación de errores adicional en la estructura de mandatos que el cliente ha enviado. Esta opción sólo debe habilitarse cuando el cliente envía al servidor solicitudes con un formato incorrecto, lo que provoca que el servidor se cuelgue. Cuando esta opción está habilitada, obtendrá un error de protocolo en lugar de que el servidor se cuelgue.

- VOLUMEHISTORY

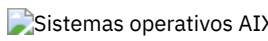
La opción VOLUMEHISTORY especifica los nombres de los archivos que se actualizarán automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor. No existe un valor predeterminado para esta opción.


Modificación de opciones del servidor

El servidor lee el archivo de opciones del servidor durante la inicialización del servidor. Cuando actualiza una opción del servidor editando el archivo, debe detener y arrancar el servidor para activar el archivo de opciones del servidor actualizado.

Acerca de esta tarea

Con el mandato SETOPT puede cambiar algunas opciones dinámicamente, sin necesidad de detener e iniciar el servidor. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica) para obtener más detalles.

 El archivo dmserv.opt.smp (que también se proporciona durante la instalación) contiene el formato del archivo de opciones y todos los valores predeterminados. Puede cambiar cualquiera de las opciones del archivo dmserv.opt.smp. Para que el servidor utilice las opciones que se han cambiado, debe cambiar el nombre del archivo por dmserv.opt. Para activar una opción del archivo de opciones del servidor, elimine el símbolo *>>> que precede a la opción. El servidor pasa por alto cualquier opción que vaya precedida del símbolo *>>>.

 Puede modificar las opciones del servidor utilizando el editor de archivos de opciones que se incluye en la consola de IBM Spectrum Protect. Este editor proporciona la detección de parámetros de comunicaciones, la validación de valores y ayuda para todas las opciones. El editor de archivos de opciones es el modo preferido de cambiar las opciones del servidor, pero también puede utilizar un editor de texto.

Tipos de opciones del servidor

Las opciones del servidor le permiten personalizar el modo en que funcionan algunas funciones y procesos.

- Opciones de comunicación del servidor
Puede utilizar las opciones del servidor para especificar los métodos de comunicaciones del servidor y sus características.
- Opciones de almacenamiento del servidor
IBM Spectrum Protect proporciona diferentes opciones que puede especificar para configurar determinadas operaciones de almacenamiento del servidor y de los dispositivos.
- Opciones de cliente/servidor
Puede utilizar las opciones de servidor para controlar el proceso de cliente/servidor.
- Opciones de fecha, número, hora e idioma
Puede utilizar las opciones de servidor para especificar los formatos de las fechas, horas, números e idioma nacional.
- Opciones de la base de datos
Puede utilizar las opciones del servidor para controlar algunos aspectos del proceso de bases de datos.
- Opciones de transferencia de datos
Puede utilizar las opciones del servidor para controlar el modo en que IBM Spectrum Protect agrupa y transfiere los datos.
- Opciones de mensajes
Puede utilizar las opciones para obtener más flexibilidad en el modo en que IBM Spectrum Protect emite los mensajes.
- Opciones de anotaciones de eventos
Opciones que pueden ayudarle a gestionar los receptores de anotaciones de eventos.
- Opciones de seguridad y del sistema de licencias
Puede utilizar las opciones del servidor para personalizar la seguridad del servidor y las auditorías de licencias.
- Opciones varias
Puede usar una serie de opciones varias para personalizar IBM Spectrum Protect.

Opciones de comunicación del servidor

Puede utilizar las opciones del servidor para especificar los métodos de comunicaciones del servidor y sus características.

Tabla 1. Opciones de comunicaciones

















Opción	Descripción
ADMINCOMMTIMEOUT	La cantidad de tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos
ADMINIDLETIMEOUT	La cantidad de tiempo que puede estar desocupada una sesión del cliente administrativo
ADMINONCLIENTPORT	Puerto que determina si las sesiones de administración pueden utilizar el puerto especificado en la opción TCPPOINT
COMMMETHOD	El método de comunicaciones del servidor
DBMTCPPOINT	El número de puerto en el que el controlador de comunicación TCP/IP para el gestor de base de datos espera las solicitudes de la sesión de cliente
DNSLOOKUP	Control de uso de Servicios de nombres de dominios para consultar nombres de sistemas que se pongan en contacto con el servidor
LDAPCACHEDURATION	Determina la cantidad de tiempo que se omiten las sesiones de autenticación, en el mismo nodo o administrador. Es posible que vea un ligero aumento de rendimiento cuando se omiten las sesiones.
LDAPURL	Especifica el servidor de directorios LDAP. Cada valor debe tener el nombre del servidor de directorios LDAP, un número de puerto y el nombre distinguido base del espacio de nombres o el sufijo que mantiene el servidor.
 Sistemas operativos Windows NAMEDPIPENAME	 Sistemas operativos Windows El método de comunicaciones de conexiones de entrada/salida nombrado
NDMPCONTROLPORT	El puerto de comunicaciones internas utilizado para determinadas operaciones NDMP (Network Data Management Protocol).
NDMPENABLEKEEPALIVE	El mecanismo de estado activo TCP
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NDMPKEEPIDLEMINUTES	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows La cantidad de tiempo de inactividad antes de que se envíe el primer paquete de estado activo TCP
 Sistemas operativos Windows NPBUFFERSIZE	 Sistemas operativos Windows El tamaño del búfer de comunicaciones de Named Pipes.

Opción	Descripción
SHMPORT	 Sistemas operativos AIX  Sistemas operativos Linux La dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida  Sistemas operativos Windows El puerto en el que el servidor está a la escucha de conexiones de memoria compartida
SNMPHEARTBEATINTERVAL	El intervalo en minutos entre consultas del servidor de IBM Spectrum Protect
SNMPMESSAGECATEGORY	Los tipos de condición de excepción utilizados cuando se reenvían los mensajes desde el servidor.
SNMPSUBAGENT	Los parámetros necesarios para que el subagente IBM Spectrum Protect se comunique con el daemon SNMP
SNMPSUBAGENTHOST	La ubicación del subagente IBM Spectrum Protect SNMP
SNMPSUBAGENTPORT	La dirección del puerto del subagente IBM Spectrum Protect SNMP
SSLFIPSMODE	Especifica si se aplica la modalidad FIPS (Federal Information Processing Standards) para la capa de sockets seguros (SSL)
SSLTCPADMINPORT	La dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL para el cliente de administración de línea de mandatos
SSLTCPPOINT	<p>El número de puerto sólo SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL procedentes de los siguientes orígenes:</p> <ul style="list-style-type: none"> • Cliente de archivado y copia de seguridad de línea de mandatos • GUI de archivado y copia de seguridad • Cliente de administración • Interfaz de programación de aplicaciones (API)
TCPADMINPORT	El número de puerto TCP/IP para las sesiones de administración
 Sistemas operativos AIX  Sistemas operativos Linux TCPBUFSIZE	 Sistemas operativos AIX  Sistemas operativos Linux El tamaño del búfer que se utiliza para las peticiones de envío TCP/IP
TCPPOINT	El número de puerto TCP/IP para las sesiones de cliente
TCPWINDOWSIZE	La ventana deslizante TCP/IP del nodo cliente

Opciones de almacenamiento del servidor

IBM Spectrum Protect proporciona diferentes opciones que puede especificar para configurar determinadas operaciones de almacenamiento del servidor y de los dispositivos.

Tabla 1. Opciones de almacenamiento del servidor

Opción	Descripción
3494SHARED	Permite compartir una biblioteca 3494 con otras aplicaciones excepto IBM Spectrum Protect.
ACSACCESSID	El ID del control de acceso de ACS.
ACSLOCKDRIVE	Permite bloquear las unidades de las bibliotecas ACSLS.
ACSQUICKINIT	Permite una inicialización rápida o completa de la biblioteca ACSLS.
ACSTIMEOUTX	El múltiplo del valor de tiempo de espera incorporado de la API ACSLS.
ASSISTVCRRECOVERY	Especifica si el servidor debe asistir a una unidad IBM 3590 a recuperarse de una condición de VCR (registros vitales de cartucho) perdidos o dañados.
CHECKTAPEPOS	Especifica si el servidor valida la posición de datos en cinta.
CLIENTDEDUPTXNLIMIT	Especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.
DEDUPREQUIRESBACKUP	Especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para optimización de almacenamiento de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.
DEDUPTIER2FILESIZE	Tamaño de archivo con el que se utiliza el procesamiento de nivel 2 para la deduplicación de datos.
DEDUPTIER3FILESIZE	Tamaño de archivo con el que se utiliza el procesamiento de nivel 3 para la deduplicación de datos.
DEVCONFIG	El archivo que almacena copias de seguridad de la información de configuración de dispositivos.
DRIVEACQUIRERETRY	El número de veces que un servidor intenta adquirir una unidad en una biblioteca IBM 349x compartida entre varias aplicaciones.
ENABLENASDEDUP	Especifica si el servidor elimina los datos duplicados almacenados por un servidor de archivos de almacenamiento conectado a red (NAS) NetApp.
NUMOPENVOLSALLOWED	El número de entradas los volúmenes FILE en una agrupación de almacenamiento deduplicada que se pueden abrir a la vez.
RECLAIMDELAY	El número de días que se retrasa la reclamación de un volumen SnapLock.
RECLAIMPERIOD	El número de días del periodo de reclamación de un volumen SnapLock
RESOURCE TIMEOUT	El intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso.
RETENTIONEXTENSION	El número de días para ampliar la fecha de retención de un volumen de SnapLock.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANDISCOVERY	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Indica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANDISCOVERYTIMEOUT	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Tiempo que transcurre antes de que el proceso de descubrimiento de SAN exceda el tiempo de espera.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANREFRESHTIME	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Tiempo que transcurre antes de renovar la información de descubrimiento de la SAN.
SEARCHMPQUEUE	El orden en que el servidor atiende las peticiones en la cola de montaje.
SERVERDEDUPTXNLIMIT	Especifica el tamaño máximo de los objeto de los que se puede optimizar el almacenamiento en el servidor.

Opciones de cliente/servidor

Puede utilizar las opciones de servidor para controlar el proceso de cliente/servidor.







Tabla 1. Opciones de cliente/servidor

Opción	Descripción
COMMTIMEOUT	El número máximo de segundos que el servidor espera a obtener una respuesta de un cliente antes de desactivar la sesión cliente por tiempo excedido.
DISABLESCHEDS	Si las planificaciones de administración y de cliente se desactivan durante una situación de recuperación del servidor de IBM Spectrum Protect.
IDLETIMEOUT	El número de minutos que el servidor permite que una sesión cliente permanezca desocupada antes de desactivar la sesión cliente por tiempo excedido.
MAXSESSIONS	El número máximo de sesiones cliente simultáneas en el servidor.
THROUGHPUTDATATHRESHOLD	El umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele tras haberse alcanzado el umbral de tiempo.
THROUGHPUTTIMETHRESHOLD	El umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.
VERBCHECK	Si se realiza una comprobación de errores adicional de los mandatos que envía el cliente

Opciones de fecha, número, hora e idioma

Puede utilizar las opciones de servidor para especificar los formatos de las fechas, horas, números e idioma nacional.

Tabla 1. Opciones de fecha, número, hora e idioma

Opción	Descripción
 Sistemas operativos Windows DATEFORMAT	 Sistemas operativos Windows El formato en el que se visualizarán las fechas
LANGUAGE	El idioma nacional que se utilizará para presentar los mensajes del cliente
 Sistemas operativos Windows NUMBERFORMAT	 Sistemas operativos Windows El formato para visualizar los números
 Sistemas operativos Windows TIMEFORMAT	 Sistemas operativos Windows El formato para visualizar la hora

Opciones de la base de datos

Puede utilizar las opciones del servidor para controlar algunos aspectos del proceso de bases de datos.

Tabla 1. Opciones de la base de datos

Opción	Descripción
ACTIVELOGDIRECTORY	Nuevo directorio de la ubicación en la que se almacenan las anotaciones activas. Utilice esta opción para cambiar la ubicación de las anotaciones activas.
ACTIVELOGSIZE	Tamaño máximo de las anotaciones activas.
ALLOWREORGINDEX	Reorganización de índice iniciada por el servidor.
ALLOWREORGTABLE	Reorganización de tabla iniciada por el servidor.
ARCHLOGDIRECTORY	El directorio en el que el gestor de bases de datos puede archivar un archivo de anotaciones una vez finalizadas todas las transacciones representadas en dicho archivo de anotaciones.
ARCHFAILOVERLOGDIRECTORY	El directorio en el que el servidor intenta almacenar los archivos de anotaciones de archivado que no pueden guardarse en el directorio de anotaciones de archivado.
DBDIAGLOGSIZE	El tamaño máximo de los archivos de registro de diagnóstico del gestor de base de datos.

Opción	Descripción
DBDIAGPATHFSTHRESHOLD	El umbral de espacio libre en el sistema de archivos o en el disco que contiene los archivos de diagnóstico del gestor de base de datos.
DBMEMPERCENT	Porcentaje de memoria del sistema que se dedica a la base de datos.
DISABLEREORGTABLE	Inhabilita la reorganización de tablas para tablas específicas.
FSUSEDTHRESHOLD	El porcentaje de sistema de archivos que puede utilizar la base de datos antes de emitir un mensaje de alerta.
MIRRORLOGDIRECTORY	El directorio para duplicar la ruta de anotaciones activas.
REORGBEGINTIME	La hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o de índice.
REORGDURATION	El intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.

Opciones de transferencia de datos

Puede utilizar las opciones del servidor para controlar el modo en que IBM Spectrum Protect agrupa y transfiere los datos.

Tabla 1. Opciones de agrupación

Opción	Descripción
MOVEBATCHSIZE	El número de archivos que se trasladarán y agruparán en un lote dentro de una transacción.
MOVESIZETHRESH	El umbral de la cantidad de datos trasladados como un lote en la misma transacción del servidor.
NDMPPORTRANGE	Dirección IP que se asocia a la interfaz en la que el servidor recibe todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
NDMPPREFDATAINTERFACE	Dirección IP que se asocia a la interfaz en la que el servidor recibe todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
REPLBATCHSIZE	El número de archivos que se van a replicar en un lote, dentro de la misma transacción de servidor.
REPLSIZETHRESH	El umbral de la cantidad de datos duplicados como un lote en la misma transacción del servidor.
TXNGROUPMAX	El número máximo de archivos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones.

Opciones de mensajes

Puede utilizar las opciones para obtener más flexibilidad en el modo en que IBM Spectrum Protect emite los mensajes.

Tabla 1. Opciones de mensajes

Opción	Descripción
EXPQUIET	Especifica si IBM Spectrum Protect envía mensajes informativos detallados durante el proceso de caducidad.
MESSAGEFORMAT	Especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.
MSGINTERVAL	El tiempo, en minutos, que debe transcurrir entre los mensajes que solicitan a un operador que monte una cinta para IBM Spectrum Protect.

Opciones de anotaciones de eventos

Opciones que pueden ayudarle a gestionar los receptores de anotaciones de eventos.









Tabla 1. Opciones de anotaciones de eventos

Opción	Descripción
EVENTSERVER	Si el servidor debe intentar establecer contacto con el servidor de eventos al arrancar el servidor.
FILEEXIT	Un archivo al que se direccionan los eventos activados (formato binario)
FILETEXTEXIT	Un archivo al que se direccionan los eventos activados (formato legible)
REPORTRETRIEVE	Registra las operaciones de restauración y recuperación de clientes.
TECBEGINEVENTLOGGING	Especifica si la anotación de eventos del receptor TIVOLI debe empezar cuando arranca el servidor.
TECHOST	Especifica el nombre de host o la dirección IP del servidor de eventos de Tivoli Enterprise Console (TEC).
TECPORT	La dirección del puerto TCP/IP en la que está conectado el servidor de eventos de Tivoli Enterprise Console.
TECUTF8EVENT	Un evento Tivoli Enterprise Console enviado desde el servidor de IBM Spectrum Protect en formato UTF8
UNIQUETDPTECEVENTS	Los eventos procedentes de un cliente de IBM Spectrum Protect Data Protection que se envían a Tivoli Enterprise Console como eventos exclusivos
UNIQUETECEVENTS	Eventos enviados a Tivoli Enterprise Console como exclusivos
USEREXIT	Salida definida por el usuario a la que se otorgará control para poder gestionar un evento

Opciones de seguridad y del sistema de licencias

Puede utilizar las opciones del servidor para personalizar la seguridad del servidor y las auditorías de licencias.

Tabla 1. Opciones de seguridad y del sistema de licencias

Opción	Descripción
 Sistemas operativos Windows ADSMGROUPNAME	 Sistemas operativos Windows El nombre de un grupo Windows
AUDITSTORAGE	Especifica que durante una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento de gestión de espacio, de copia de seguridad/archivado que está utilizándose.
BACKUPINITIATIONROOT	Especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.
LDAPURL	Especifica el servidor de directorios LDAP. Cada valor debe tener el nombre del servidor de directorios LDAP, un número de puerto y el nombre distinguido base del espacio de nombres o el sufijo que mantiene el servidor.
 Sistemas operativos Windows NPAUDITFAILURE	 Sistemas operativos Windows Especifica que un nodo sólo puede acceder a sus propios datos.
 Sistemas operativos Windows NPAUDITSUCCESS	 Sistemas operativos Windows Especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.
QUERYAUTH	El nivel de autorización de administración necesario para emitir los mandatos QUERY o SQL SELECT.
REQSYSAUTHOUTFILE	Especifica si es necesaria la autorización del sistema para los mandatos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo.
 Sistemas operativos Windows SECUREPIPES	 Sistemas operativos Windows Con el protocolo Named Pipes, especifica que el servidor comprueba el grupo Windows a fin de autenticar un cliente.
SHREDDING	Especifica si la fragmentación de datos confidenciales suprimidos se hace de forma automática o manual

Referencia relacionada:

Opciones de comunicación del servidor

Opciones varias

Puede usar una serie de opciones varias para personalizar IBM Spectrum Protect.

Tabla 1. Opciones varias

Opción	Descripción
ALIASHALT	Permite a los administradores asignar un nombre diferente a un mandato HALT de IBM Spectrum Protect.
DISPLAYLFINFO	Especifica si los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del agente de almacenamiento
EXPINTERVAL	El intervalo entre procesos de caducidad de inventario automáticas
FFDCLOGNAME	El nombre para el registro FFDC (first failure data capture)
FFDCMAXLOGSIZE	El tamaño máximo del registro FFDC (First Failure Data Capture)
NOPREEMPT	Especifica que ninguna operación puede adelantarse a otra para acceder a un volumen y que únicamente una operación de copia de seguridad de base de datos puede adelantarse a otra operación para acceder a un dispositivo.
NORETRIEVEDATE	Especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo.
RESTOREINTERVAL	Intervalo de tiempo durante el que se puede guardar una sesión de restauración reinicializable en la base de datos del servidor.
VOLUMEHISTORY	El archivo que se actualizará automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor.

3494SHARED

La opción 3494SHARED especifica si una biblioteca IBM® 3494 puede compartir aplicaciones distintas de IBM Spectrum Protect.

El valor predeterminado es NO, que significa que la biblioteca 3494 no se puede compartir con ninguna otra aplicación excepto IBM Spectrum Protect. Si establece esta opción en YES, IBM Spectrum Protect determina para cada petición de montaje si se están utilizando las unidades. Una vez realizada la consulta, IBM Spectrum Protect selecciona una unidad disponible que no utilice otra aplicación. Sólo debe activarse la posibilidad de compartir si en la biblioteca hay más de dos unidades. Si actualmente comparte una biblioteca IBM 3494 con otras aplicaciones, debe especificar esta opción.

Sintaxis

```
>>-3494SHARED--+-Yes+-----<<  
                '-No--'
```

Parámetros

Yes

- No Especifica que otras aplicaciones pueden compartir la biblioteca 3494.
- No Especifica que ninguna otra aplicación puede compartir la biblioteca 3494.

Ejemplos

Activar el compartimiento de una biblioteca 3494:

```
3494shared yes
```

ACSACCESSID

La opción ACSACCESSID especifica el identificador del control de acceso de ACS para una biblioteca ACSLS.

Sintaxis

```
>>-ACSACCESSID--nombre-----<<
```

Parámetros

nombre

Especifica un identificador de 1 a 64 caracteres. El identificador predeterminada es el nombre de host local.

Ejemplos

```
acsaccessid region
```

ACSLOCKDRIVE

La opción ACSLOCKDRIVE especifica si las unidades de las bibliotecas ACSLS están bloqueadas. Al bloquear las unidades, se garantiza el uso exclusivo de la unidad de la biblioteca ACSLS en un entorno compartido. Sin embargo, el rendimiento es mejor si las bibliotecas no se bloquean. Cuando otras aplicaciones no comparten las unidades de IBM Spectrum Protect, no es necesario bloquear las unidades.

Sintaxis

```
>>-ACSLOCKDRIVE--+-Yes-+-----<<  
                '-No--'
```

Parámetros

Yes

Especifica que las unidades están bloqueadas.

No

Especifica que las unidades no están bloqueadas.

Ejemplos

```
acslockdrive yes
```

ACSQUICKINIT

La opción ACSQUICKINIT especifica si, en el arranque del servidor, la inicialización de la biblioteca ACSLS es rápida o completa. El valor predeterminado es Yes. Una inicialización rápida evita la sobrecarga asociada con la sincronización del inventario del servidor de IBM Spectrum Protect con el inventario de biblioteca ACSLS (mediante una auditoría de la biblioteca).

Sintaxis

```
>>-ACSQUICKINIT--+-Yes-+-----><
      '-No--'
```

Parámetros

Yes

Especifica que se lleve a cabo una inicialización rápida de la biblioteca ACSLS. Cuando la opción se establece en Yes, IBM Spectrum Protect omite la verificación del inventario de biblioteca, e inicializa rápidamente la biblioteca haciendo que IBM Spectrum Protect pueda disponer de la misma antes que si se llevara a cabo una inicialización completa.

Esta opción debe establecerse en Yes cuando se sabe que el inventario de biblioteca física y el inventario de biblioteca de IBM Spectrum Protect no han cambiado y que no es necesario realizar una auditoría.

No

Especifica que se lleve a cabo una inicialización completa de la biblioteca ACSLS y del inventario de biblioteca. Cuando la opción se establece en No, IBM Spectrum Protect sincroniza su inventario de volúmenes de la biblioteca con lo que notifica el gestor de bibliotecas ACSLS.

Ejemplos

```
acsquickinit yes
```

ACSTIMEOUTX

La opción ACSTIMEOUTX especifica el múltiplo del valor de tiempo de espera incorporado de las API ACSLS. El valor de tiempo de espera incorporado de la API de introducción, expulsión y auditoría ACS son 1800 segundos; el valor de todas las demás API ACSLS son 600 segundos. Por ejemplo, si el múltiplo especificado es 5, el valor de tiempo de espera de la API de auditoría serán 9000 segundos y el valor de todas las demás API serán 3000 segundos.

Sintaxis

```
>>-ACSTIMEOUTX--valor-----><
```

Parámetros

valor

Especifica el múltiplo del valor de tiempo de espera incorporado de la API ACSLS. El rango es de 1 a 100. El valor predeterminado es 1.

Ejemplos

```
acstimeoutx 1
```

ACTIVELOGDIRECTORY

La opción ACTIVELOGDIRECTORY especifica el nombre del directorio donde están almacenados todos los registros activos.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT. En condiciones generales de utilización, no es necesario cambiar la opción. Consulte el apartado DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones) para obtener ayuda para esta opción.

Sintaxis

```
>>-ACTIVELOGDirectory--dir_name-----><
```

Parámetros

nombre_dir

Especifica un nombre de directorio cualificado al completo. El directorio debe existir, debe estar vacío, y debe ser accesible mediante el ID de usuario del gestor de base de datos. Si cambia el directorio de anotaciones activas, IBM Spectrum Protect moverá las anotaciones activas existentes a la ubicación que este directorio especifica. El número máximo de caracteres es 175.

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
activedirectory /tsm/activedir
```

 Sistemas operativos Windows

```
activedirectory c:\tsmserv1\activedir
```

ACTIVELOGSIZE

La opción ACTIVELOGSIZE establece el tamaño total del registro.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSEV FORMAT. En condiciones generales de utilización, no es necesario cambiar la opción. Consulte el apartado DSMSEV FORMAT (Dar formato a la base de datos y a las anotaciones) para obtener ayuda para esta opción.

Sintaxis

```
.-16GB-----.  
>>-ACTIVELOGSize--+-megabytes-+-----<<
```

Parámetros

megabytes

Especifica el tamaño del archivo de anotaciones activas en megabytes. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16.384 MB (16 GB).

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Ejemplos

```
activesize 8192
```

ADMINCOMMTIMEOUT

La opción ADMINCOMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos.

Si el tiempo supera este periodo de tiempo de espera, el servidor finaliza la sesión con el cliente administrativo. Puede aumentar el valor de tiempo de espera para evitar que las sesiones de los clientes administrativos excedan el tiempo de espera.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
                .-60-----.  
>>-ADMINCOMMTIMEOUT--+-segundos+-----<<
```

Parámetros

seconds

Especifica el número máximo de segundos que el servidor espera una respuesta del cliente administrativo. El valor predeterminado es 60. El valor mínimo es 1.

Ejemplos

```
admincommtimeout 60
```

ADMINIDLETIMEOUT

La opción ADMINIDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente administrativo puede estar desocupada antes de que la cancele el servidor.

Si hay una gran carga de red en el entorno, puede aumentar el valor de tiempo de espera para evitar que los clientes administrativos excedan el tiempo de espera. No obstante, una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
                .-15-----.  
>>-ADMINIDLETIMEOUT--+-minutos+-----<<
```

Parámetros

minutos

Especifica el número máximo de minutos que el servidor espera a un cliente administrativo desocupado. El valor predeterminado es de 15 minutos. El valor mínimo es de 1 minuto.

Ejemplos

```
adminidletimeout 20
```

ADMINONCLIENTPORT

La opción ADMINONCLIENTPORT especifica si las sesiones administrativas pueden utilizar TCPPOINT. El valor predeterminado es YES.

Sintaxis

```
>>-ADMINONCLIENTPORT--+-YES+-----<<  
                        '-NO--'
```

Parámetros

YES

Si la opción está establecida en YES, o si TCPPOINT y TCPADMINPORT tienen el mismo valor (es así de forma predeterminada), las sesiones administrativas pueden utilizar TCPPOINT.

NO

Si la opción está establecida en NO, y si el valor de TCPADMINPORT es distinto del valor TCPPOINT, las sesiones administrativas no pueden utilizar TCPPOINT.

Ejemplos

Especificar que las sesiones de administración pueden utilizar TCPPOINT.

```
adminonclientport yes
```

 Sistemas operativos Windows

ADSMGROUPNAME

La opción ADSMGROUPNAME especifica el nombre de un grupo Windows. Un nodo cliente debe ser miembro de este grupo para poder utilizar el servidor de IBM Spectrum Protect a través de NT Unified Logon. El nodo de cliente también debe ser un nodo de cliente de IBM Spectrum Protect registrado.

Sintaxis

```
>>-ADSMGROUName--nombre_grupo-----<<
```

Parámetros

nombre_grupo
Especifica un nombre de grupo Windows.

Ejemplos

Especificar IDD como un grupo Windows:

```
adsmgroup idd
```

ALIASHALT

La opción ALIASHALT permite a los administradores asignar un nombre diferente a un mandato **HALT** de IBM Spectrum Protect.

El cliente de administración reconoce un alias para el mandato HALT cuando el cliente se inicia habiéndose especificado la opción CHECKALIASHALT. Consulte el apartado Opciones de cliente de administración para obtener más detalles.

Sintaxis

```
>>-ALIASHALT--nombre_nuevo-----<<
```

Parámetros

nombre_nuevo
Especifica el alias del mandato HALT para concluir el servidor de IBM Spectrum Protect. La longitud mínima de *nombre_nuevo* es 1 y la máxima de 16.

Ejemplos

```
aliashalt tsmhalt
```

ALLOWDESAUTH

La opción ALLOWDESAUTH especifica si se debe permitir la utilización del algoritmo DES (Data Encryption Standard) para la autenticación entre un servidor y un cliente de archivado y copia de seguridad.

Para impedir la utilización de DES, especifique el valor NO para la opción ALLOWDESAUTH.

Para configurar el servidor de IBM Spectrum Protect para que esté en conformidad con el estándar NIST SP800-131A, establezca esta opción en NO.

Restricciones:

- El cliente de archivado y copia de seguridad debe estar ejecutando la versión 6.3 o posterior si se autentica en un servidor con la opción ALLOWDESAUTH establecida en NO.
- El despliegue automático del cliente de archivado y copia de seguridad falla si esta opción está establecida en NO.

Sintaxis

```
.-ALLOWDESAUTH--Yes-----.  
>>+-----+-----><  
'-ALLOWDESAUTH---+No--+-'  
      '-Yes-'
```

Parámetros

Yes

Especifica que el servidor permite la autenticación con los clientes de archivado y copia de seguridad que utilizan cifrado basado en DES. El valor predeterminado es YES.

No

Especifica que el servidor rechaza los clientes de archivado/copia de seguridad que intentan autenticarse con cifrado basado en DES.

Ejemplos

Especificar que el servidor rechace los clientes de archivado/copia de seguridad que intentan autenticarse con cifrado basado en DES:

```
allowdesauth no
```

Especificar que el servidor permita la autenticación con los clientes de archivado/copia de seguridad que utilizan cifrado basado en DES:

```
allowdesauth yes
```

ALLOWREORGINDEX

La opción ALLOWREORGINDEX especifica si la reorganización de índice iniciada por el servidor está activada o desactivada.

El valor predeterminado es YES.

Sintaxis

```
>>-ALLOWREORGINDEX---+Yes+-----><  
      '-No--'
```

Parámetros

Yes

Especifica que la reorganización de índice iniciada por el servidor está activada.

No

Especifica que la reorganización de índice iniciada por el servidor no está activada.

Ejemplo

Especificar que la reorganización de índice iniciada por el servidor está activada.

```
allowreorgindex yes
```

ALLOWREORGTABLE

La opción ALLOWREORGTABLE especifica si la reorganización de tabla iniciada por el servidor está activada o desactivada.

El valor predeterminado es YES.

Sintaxis

```
>>-ALLOWREORGTABLE---+-Yes+-----<<
                        '-No--'
```

Parámetros

Yes

Especifica que la reorganización de tabla iniciada por el servidor está activada.

No

Especifica que la reorganización de tabla iniciada por el servidor no está activada.

Ejemplos

Especifique que la reorganización de tabla iniciada por el servidor no está activada.

```
allowreorgtable no
```

ARCHFAILOVERLOGDIRECTORY

La opción ARCHFAILOVERLOGDIRECTORY especifica el directorio que utiliza el servidor para almacenar los archivos de registro de archivado que no se pueden almacenar en el directorio de registros de archivado.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSErv FORMAT. Normalmente no es necesario cambiar el directorio.

Sintaxis

```
>>-ARCHFailoverlogdirectory--dir_name-----<<
```

Parámetros

nombre_dir

Especifica un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
archfailoverlogdirectory /tsm/archfailoverlog
```

 Sistemas operativos Windows

```
archfailoverlogdirectory c:\tsmserv1\archfailoverlog
```

ARCHLOGCOMPRESS

Puede habilitar o inhabilitar la compresión de registros de archivado en el servidor de IBM Spectrum Protect. Al comprimir los registros de archivado, se reduce la cantidad de espacio necesaria para el almacenamiento.

La opción del servidor ARCHLOGCOMPRESS especifica si se comprimen archivos de registro en que se graban en el directorio de archivado para registros.

Sintaxis

```
>>-ARCHLOGCOMPRESS---+-No-- .
                        '+-----<<
                        '-Yes-'
```

Parámetros

No

Especifica que los archivos que se graban en el directorio del registro de archivado no se comprimen. El valor predeterminado es No.

Yes

Especifica que los archivos que se graban en el directorio del registro de archivado se comprimen.

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción del servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

Ejemplo

Para permitir la compresión de archivos de registro que se graban en el directorio de registro de archivado, especifique la opción siguiente:

```
archlogcompress yes
```

ARCHLOGDIRECTORY

La opción ARCHLOGDIRECTORY especifica un directorio en el que el gestor de base de datos puede archivar un archivo de registro una vez completadas todas las transacciones representadas en dicho archivo de registro.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT.

Sintaxis

```
>>-ARCHLOGDirectory--dir_name-----<<
```

Parámetros

nombre_dir

Especifica un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
archlogdirectory /tsm/archlog
```

 Sistemas operativos Windows

```
archlogdirectory d:\tmserv1\archlog
```

ARCHLOGUSEDTHRESHOLD

La opción ARCHLOGUSEDTHRESHOLD especifica cuándo iniciar una copia de seguridad de base de datos automática en relación con el porcentaje de espacio de archivo de anotaciones de archivado utilizado. El valor predeterminado es el 80 por ciento.

La opción ARCHLOGUSEDTHRESHOLD impide copias de seguridad automáticas frecuentes. Por ejemplo, si el directorio de archivos de registro de archivado reside en un sistema de archivos o la unidad de 400 GB, se realizará una copia de seguridad de la base de datos si hay menos de 80 GB de espacio libre. Las copias de seguridad de la base de datos hacen que el servidor utilice una cantidad excesiva de cintas reutilizables.

Sintaxis

.-80----.

```
>>-ARCHLOGUSEDTHRESHOLD--+-valor+-----<<
```

Parámetros

valor

El porcentaje de espacio de archivo de registro de archivado utilizado antes de que empiece la copia de seguridad.

Especifique para iniciar una copia de seguridad automática cuando se haya utilizado el 90 por ciento de espacio de archivos de registro de archivado.

```
archlogusedthreshold 90
```

ASSISTVCRRECOVERY

La opción ASSISTVCRRECOVERY especifica si IBM Spectrum Protect debe ayudar a una unidad IBM® 3590 a recuperarse de una condición de VCR (Vital Cartridge Records) perdidos o dañados. Si especifica YES (el valor predeterminado) y si IBM Spectrum Protect detecta un error durante el proceso de montaje, se sitúa al final de los datos durante el proceso de desmontaje para permitir que las unidades restauren el VCR. Durante la operación de cinta, es posible que se produzca un pequeño efecto sobre el rendimiento ya que la unidad no puede realizar una búsqueda rápida con un VCR perdido o dañado. Sin embargo, no se produce ninguna pérdida de datos.

Sintaxis

```
>>-ASSISTVCRREcovery--+-Yes+-----<<  
      '-No--'
```

Parámetros

Yes

Especifica que el servidor proporcionará ayuda para la recuperación.

No

Especifica que el servidor no proporcionará ayuda para la recuperación.

Ejemplos

Desactivar la ayuda para la recuperación:

```
assistvcrrecovery no
```

AUDITSTORAGE

Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento del servidor utilizado para operaciones de copia de seguridad y archivado, y para archivos bajo gestión de espacio. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de CPU y puede detener otras actividades del servidor. Puede utilizar la opción AUDITSTORAGE para especificar que el almacenamiento no se ha de calcular como parte de una auditoría de licencias.

Nota: Esta opción anteriormente se llamaba NOAUDITSTORAGE.

Sintaxis

```
>>-AUDITStorage--+-Yes+-----<<  
      '-No--'
```

Parámetros

Yes

Especifica que el almacenamiento se calculará como parte de una auditoría de licencias. El valor predeterminado es Yes.

No

Especifica que el almacenamiento no se calculará como parte de una auditoría de licencias.

Ejemplos

```
auditstorage yes
```

BACKUPINITIATIONROOT

La opción BACKUPINITIATIONROOT especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-BACKUPINITIATIONROOT--+-ON---+-----+-----<<  
      '-OFF-'
```

Parámetros

ON

Especifica las sesiones de los clientes en los sistemas operativos AIX, Linux, Mac OS X y Solaris, en las que los usuarios que no son usuarios autorizados de IBM Spectrum Protect no puede iniciar operaciones de copia de seguridad. Este es el valor predeterminado. El servidor sustituye el valor del servidor para el parámetro BACKUPINITIATION que se especifica en los mandatos REGISTER NODE y UPDATE NODE.

Consejo: Para obtener una visión general de los usuarios autorizados de IBM Spectrum Protect, consulte la sección Cliente raíz de UNIX y Linux y tareas de usuario autorizadas.

OFF

Especifica que se utiliza el valor del nodo para el parámetro BACKUPINITIATION. El parámetro BACKUPINITIATION se especifica en los mandatos REGISTER NODE y UPDATE NODE.

Ejemplo

Especifique que se ha de utilizar el valor del nodo para el parámetro BACKUPINITIATION.

```
backupinitiationroot off
```

CHECKTAPEPOS

La opción CHECKTAPEPOS especifica si el servidor de IBM Spectrum Protect valida la posición de los bloques de datos en la cinta.

La opción CHECKTAPEPOS se aplica solo a operaciones que utilizan unidades de cintas. No se aplica a clases de dispositivos de acceso secuencial que no sean de cinta, como por ejemplo FILE. Si la información del servidor sobre la posición no coincide con la posición detectada por la unidad, se muestra un mensaje de error, la transacción se retrotrae y los datos no se confirman en la base de datos.

Utilizando la opción CHECKTAPEPOS puede habilitar la modalidad de sólo agregar para las unidades IBM LTO Generation 5 y posteriores y para cualquier unidad que dé soporte a esta característica. Cuando está activada, la unidad emite un error después de recibir instrucciones de sobrescribir los datos en el volumen montado actualmente. El servidor de IBM Spectrum Protect vuelve a colocar la cinta en el bloque correcto y continúa escribiendo datos. La modalidad de sólo agregar ofrece una protección agregada al impedir la mayoría de situaciones de sobrescritura de datos. Si utiliza una unidad que da soporte a esta característica, puede validar la posición de los datos en la cinta utilizando IBM Spectrum Protect y la unidad, o puede activar una opción o la otra.

Nota: Al utilizar las funciones de aceleración de cinta SAN en Fabric, establezca CHECKTAPEPOS en DRIVEonly o No para evitar errores de posicionamiento falso positivo. La opción de servidor IBM Spectrum Protect CHECKTAPEPOS no requiere que una unidad con posibilidad de sólo agregar.

Los cambios en la opción CHECKTAPEPOS sólo afectan a los montajes una vez completada la actualización a la unidad.

El valor predeterminado es YES.

Sintaxis

```
>>-CHECKTAPEPOS--+-Yes-----+-----<<
```

```
+-No-----+
+-TSMonly---+
'-DRIVEonly-'
```

Parámetros

Yes

Especifica que el servidor de IBM Spectrum Protect valida la posición de datos en la cinta. Para las unidades que dan soporte a la modalidad de sólo agregar, este parámetro especifica que IBM Spectrum Protect permite a la unidad validar también la posición de los datos durante cada operación WRITE para impedir la sobrescritura de estos. El valor predeterminado es Yes.

No

Especifica que la validación de la posición de todos los datos está desactivada.

TSMonly

Especifica que el servidor de IBM Spectrum Protect valida la posición de datos en la cinta. El servidor no utiliza la modalidad de sólo agregar aunque la unidad dé soporte a la característica.

DRIVEonly

Especifica que el servidor de IBM Spectrum Protect activa la modalidad de sólo agregar para las unidades que dan soporte a esta característica. El servidor no valida la posición de los datos en la cinta.

Ejemplo

Valide la posición de los datos en la cinta y active la modalidad de sólo agregar para una unidad soportada:

```
checktapepos yes
```

CLIENTDEDUPTXNLIMIT

La opción CLIENTDEDUPTXNLIMIT especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.

Cuando se usa optimización de almacenamiento en el lado del cliente para objetos de gran tamaño, puede producirse una actividad intensiva en la base de datos por las transacciones de ejecución larga necesarias para actualizar dicha base de datos. Unos niveles altos de actividad de la base de datos pueden producir los siguientes síntomas:

- Rendimiento reducido para las operaciones de copia de seguridad y de archivado del cliente
- Contienda de recursos debido a operaciones simultáneas del servidor
- Actividad excesiva del registro de recuperación

La medida en que se producen estos síntomas depende del número y del tamaño de los objetos que se almacenan utilizando optimización de almacenamiento por el cliente, la intensidad y el tipo de las operaciones que tienen lugar en el servidor de IBM Spectrum Protect y la configuración de servidor de IBM Spectrum Protect.

Con la opción de servidor CLIENTDEDUPTXNLIMIT es posible especificar un tamaño máximo, en gigabytes, para las transacciones cuando se realizan copias de seguridad o se archivan los datos del cliente con almacenamiento optimizado. Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por CLIENTDEDUPTXNLIMIT, dichos objetos no tienen optimización del almacenamiento por parte del cliente y la transacción puede fallar. Es posible especificar un valor de 32 a 102400 GB. El valor predeterminado es 5120 GB.

Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por CLIENTDEDUPTXNLIMIT, los objetos o el conjunto de objetos no tienen optimización del almacenamiento por parte del cliente. Sin embargo, los objetos se envían al servidor. Estos objetos pueden tener optimización de almacenamiento en el servidor, en función de si la agrupación de almacenamiento de destino está configurada para dicha optimización y del valor de la opción SERVERDEDUPTXNLIMIT. Los objetos en una agrupación de almacenamiento con optimización de almacenamiento habilitada inferiores al valor de SERVERDEDUPTXNLIMIT sí se optimizan mediante un proceso de identificación de duplicación del servidor.

El valor adecuado para esta opción depende de la configuración de servidor de IBM Spectrum Protect y de la actividad simultánea del servidor. Es posible especificar un valor alto para esta opción si se minimiza la contienda de recursos. Para minimizar la contienda de recursos, realice operaciones como copia de seguridad, archivado, identificación de duplicados (el mandato IDENTIFY DUPLICATES) y reclamación en distintos momentos.

Para actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor, utilice el mandato SETOPT.

Sintaxis

```
.-5120-----.  
>>-CLIENTDEDUPTXNlimit--+gigabytes+-----<<
```

Parámetros

gigabytes

Especifica el tamaño máximo, en gigabytes, de los objetos de los que se pueden archivar o hacer copia de seguridad usando optimización de almacenamiento de datos en el lado del cliente. Es posible especificar un valor de 32 a 102400. El valor predeterminado es 5120.

Ejemplos

Inhabilitar la optimización de almacenamiento de datos en el lado del cliente para todos los objetos de más de 80 GB:

```
clientdeduptxnlimit 80
```

CLIENTDEPLOYCATALOGURL

La opción CLIENTDEPLOYCATALOGURL especifica la ubicación del archivo de catálogo que se utiliza para las operaciones de despliegue de cliente automático.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-CLIENTDEPLOYCATalogurl----->  
.-https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json-  
>--+url-----+<<
```

Parámetros

url

Especifica el URL Desde que el servidor descarga el archivo de catálogo para las operaciones de despliegue de cliente automático. El archivo de catálogo almacena propiedades para las operaciones de despliegue del cliente, incluida la ubicación de los paquetes de despliegue. El URL predeterminado es <https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json>.

Para especificar que el archivo de catálogo se descarga desde otro lugar, utilice el mandato SETOPT para especificar un URL personalizado. Para restablecer el URL a su valor predeterminado, utilice el mandato SETOPT con una cadena vacía: "". Si especifica un URL personalizado, dicho URL se retendrá una vez actualizado el servidor.

Ejemplo

Especificar un URL personalizado de <https://direcciónPersonalizada>.

```
setopt clientdeploycatalogurl https://direcciónPersonalizada
```

Ejemplo

Restaurar la opción CLIENTDEPLOYCATALOGURL a su valor predeterminado.

```
setopt clientdeploycatalogurl ""
```

CLIENTDEPLOYUSELOCALCATALOG

La opción CLIENTDEPLOYCATALOGURL especifica si la versión local del archivo de catálogo se utiliza para las operaciones de despliegue de cliente automático.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
.-No--.  
>>-CLIENTDEPLOYUSELOCALcatalog--+-Yes-+-----><
```

Parámetros

No

Especifica que la versión local del archivo de catálogo no se utiliza. En su lugar, el archivo de catálogo se descarga desde la ubicación que se especifica mediante la opción CLIENTDEPLOYCATALOGURL. El valor predeterminado es NO.

Sí

Especifica que se utiliza la versión local del archivo de catálogo. Los archivos de catálogo no se descargan durante las operaciones de despliegue del cliente. Si se establece esta opción en YES, el valor se retiene después de actualizarse el servidor.

Ejemplo

Especifica que se utiliza la versión local del archivo de catálogo.

```
setopt clientdeployuselocalcatalog yes
```

COMMETHOD

La opción COMMETHOD especifica el método de comunicaciones que utilizará el servidor.

Puede configurar el servidor para que utilice varios métodos de comunicaciones. Los métodos de comunicaciones que se utilizan con más frecuencia son TCPIP, V6TCPIP y SHAREDMEM. Para especificar varios métodos de comunicaciones, habilite cada método agregando una stanza COMMETHOD al archivo de opciones dsmserv.opt.


Importante: Cuando habilita un método de comunicaciones, también debe añadir al archivo de opciones las opciones específicas del método de comunicaciones.


Sintaxis

```
.-TCPIP-----.  
>>-COMMMethod--+-NAMEDPIPE-+-----><  
+-NONE-----+  
+-SHAREDMEM-+  
+-SNMP-----+  
+-TCPIP-----+  
'-V6TCPIP---'
```

Parámetros

Puede seleccionar uno de los siguientes métodos de comunicaciones:

 Sistemas operativos Windows NAMEDPIPES

 Sistemas operativos Windows Especifica la opción del método de comunicaciones de conexiones de entrada/salida nombrado.

NONE

Especifica que no se utilizará ningún método de comunicaciones. Esta opción no permite a los usuarios conectarse con el servidor y resulta útil para experimentar con mandatos de política.

SHAREDMEM

Especifica la opción del método de comunicaciones de memoria compartida. Este método utiliza la misma área de memoria para enviar datos entre varias aplicaciones a la vez. Tanto el servidor como el cliente de archivado y copia de seguridad deben estar configurados para dar soporte al método de comunicación de memoria compartida y deben estar instalados en el mismo sistema.

SNMP

Especifica la opción del método de comunicaciones SNMP.

TCPIP

Especifica la opción del método de comunicaciones TCP/IP. Esta opción es la opción predeterminada. Si se especifica TCPIP, solamente se utiliza TCP/IP Versión 4.

V6TCPIP

Especifica la opción del método de comunicaciones TCP/IP. Si TCP/IP Versión 4 y Versión 6 están configuradas, IBM Spectrum Protect utiliza simultáneamente ambos protocolos. Si se especifican COMMMETHOD TCPIP y COMMMETHOD V6TCPIP, V6TCPIP prevalece sobre la especificación de TCPIP. Debe haber un entorno de servidor de nombres de dominio (DNS) para utilizar TCP/IP V4 o TCP/IP V6 si se especifica esta opción.

Ejemplos

Ejemplo de especificación de métodos de comunicación que va a utilizar el servidor (TCP/IP y TCP/IP versión 6):

```
commmethod tcpip  
commmethod v6tcpip
```

COMMTIMEOUT

La opción COMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente durante una operación que produce una actualización de la base de datos. Si el tiempo supera este tiempo de espera, el servidor finaliza la sesión con el cliente. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera. Los clientes pueden exceder el tiempo de espera si existe una gran carga de red en el entorno o realizan copias de seguridad de archivos grandes.

La opción de servidor COMMTIMEOUT se utiliza en las sesiones no administrativas. Consulte la opción ADMINCOMMTIMEOUT para las sesiones de cliente administrativas.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Sintaxis

```
.-60-----.  
>>-COMMTIMEOUT--+-segundos+-----<<
```




Parámetros

seconds

Especifica el número máximo de segundos que el servidor espera una respuesta del cliente. El valor predeterminado es 60. El valor mínimo es 1.

Ejemplos

```
commtimeout 60
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

CONTAINERRESOURCETIMEOUT

La opción CONTAINERRESOURCETIMEOUT especifica durante cuánto tiempo espera el servidor a completar una operación de almacén de datos en una agrupación de almacenamiento de contenedor.

Sintaxis

Cuando se excede el tiempo de espera, los datos almacenados en la agrupación de almacenamiento de contenedor se conservan. La operación de almacenamiento de datos finaliza y se cancela la solicitud para el recurso de contenedor.

```
.-180-----.  
>>-CONTAINERRESOURCETIMEOUT--+-minutos+-----<<
```

Parámetros


minutos

Especifica el número máximo de minutos que espera el servidor antes de que se cancele una operación. El valor predeterminado es de 180 minutos. El valor mínimo es de 1 minuto.

Ejemplo

Especifique que el servidor ha de esperar 4 horas antes de que se cancele una operación de almacenamiento de datos en una agrupación de almacenamiento de contenedor.

```
containerresourcetimeout 240
```

 Sistemas operativos Windows

DATEFORMAT

La opción DATEFORMAT especifica el formato que el servidor ha de utilizar para visualizar las fechas.

El formato del entorno local altera temporalmente el valor DATEFORMAT si el entorno local se inicializa durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

Sintaxis

```
>>-DATEformat--n-----<<
```

Parámetros

n
Seleccione un número de 1 a 5 para identificar el formato de fecha que utiliza el servidor. El valor predeterminado es 1.

1	MM/DD/AAAA
2	DD-MM-AAAA
3	AAAA-MM-DD
4	DD.MM.AAAA
5	AAAA.MM.DD

Ejemplos

```
dateformat 4
```

DBDIAGLOGSIZE

Esta opción permite controlar el espacio que utilizan los archivos de registro de diagnóstico.

El gestor de base de datos utiliza archivos de registro de diagnóstico para registrar mensajes. Debe controlar el tamaño de los archivos de registro para que no se llene el sistema de archivos. Utilice la opción DBDIAGLOGSIZE para establecer la cantidad de espacio que utilizan los archivos de registro.

Si establece un valor del 2 al 9999, se retiene un máximo de 10 archivos de registro de diagnóstico rotatorios. Cada nombre de archivo indica el orden en que se ha creado. Cuando un archivo se llena, se crea el siguiente archivo. Cuando se llena el décimo archivo, se suprime el archivo más antiguo y se crea un nuevo archivo. A continuación, se muestra un ejemplo de cómo serían los archivos de registro rotatorios:

```
db2diag.14.log, db2diag.15.log, ... , db2diag.22.log, db2diag.23.log
```

Cuando db2diag.23.log está lleno, se suprime db2diag.14.log y se crea db2diag.24.log.

El servidor comprueba el espacio de archivo que contiene los archivos de registro de diagnóstico cada hora. Aparecen mensajes cada 12 horas si se produce alguna de las siguientes condiciones:

- El espacio disponible en el sistema de archivos donde se encuentran los archivos de registro de diagnóstico es menor del 20% del espacio del sistema de archivos total.
- El espacio disponible en el sistema de archivos donde se encuentra el directorio de la instancia de servidor es menor que 1 GB.

Si especifica el valor 0, sólo se utiliza un archivo de registro, db2diag.log, para todos los mensajes de diagnóstico. No se imponen límites sobre el tamaño del archivo de registro.

Restricción: Debe supervisar el tamaño de los archivos de registro para asegurarse de que no utilizan todo el espacio disponible en el sistema de archivos. Si no hay suficiente espacio disponible, es posible que el servidor deje de responder.

Sintaxis

```
                .-1024-----.  
>>-DBDIAGLOGSize--+-megabytes-+-----<<
```

Parámetros

megabytes

Especifica el espacio que utilizan los archivos de registro de diagnóstico en megabytes. Especifique un valor del 2 al 9999, o bien el valor 0. El valor predeterminado es 1024.

Si especifica un valor del 2 al 9999, se utilizan archivos de registro rotatorios y el valor especifica el tamaño en megabytes de los 10 archivos en total. El valor se restablece a 1024 siempre que se reinicia el servidor.

Si especifica el valor 0, se utiliza un archivo de registro y no se impone ningún límite sobre su tamaño.

Si desea archivar mensajes, especifique el valor 0 para asegurarse de que el archivo db2diag.log puede utilizar todo el espacio disponible sin utilizar los archivos de registro rotativos.

Después de establecer el valor del parámetro megabytes en 0 utilizando la opción DBDIAGLOGSIZE, los mensajes se graban inicialmente en los archivos de registro rotativos. Tras reiniciar el servidor, los mensajes se graban en el archivo db2diag.log.

Consejo: Si especifica un valor del 2 al 9999 utilizando el archivo de opciones de servidor, dsmserv.opt, el valor no se reinicia automáticamente al iniciar el servidor. El valor sigue siendo el mismo hasta que se cambia o se elimina del archivo dsmserv.opt con el mandato SETOPT.

Ejemplo: especificar un tamaño máximo de 5120 megabytes

Especificar el tamaño de los archivos de registro de diagnóstico en 5120 megabytes (5 GB):

```
dbdiaglogsize 5120
```

Ejemplo: archivar los mensajes en un único archivo de registro

Archivar los mensajes especificando que éstos se graban en el archivo db2diag.log:

```
dbdiaglogsize 0
```

Información relacionada:

[Información del producto DB2 V10.5](#)

DBDIAGPATHFSTHRESHOLD

La opción DBDIAGPATHFSTHRESHOLD especifica un umbral para el espacio libre en el sistema de archivos o disco que contiene el archivo db2diag.log.

Cuando la cantidad de espacio libre es igual o menor que el umbral especificado, se muestra el mensaje de error ANR1545W. De forma predeterminada, el mensaje se muestra cuando el sistema de archivos o el disco tiene un 20% o menos de espacio de disco libre.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-DBDIAGPATHFSTHreshold--percent-----<<
```

Parámetro

porcentaje

Especifica el porcentaje de espacio disponible en el sistema de archivos. Los valores válidos están en el rango de 0 - 100. El valor predeterminado es 20.

Consejo: Para obtener mejores resultados, no configure un valor superior o inferior percent para el parámetro. Un valor bajo puede hacer que el sistema de archivos se llene antes de que pueda corregir el problema. Un sistema de archivos lleno puede

dañar la base de datos del servidor. Un valor alto podría dar como resultado muchos mensajes ANR1545W en el registro de actividad del servidor.

Ejemplo

Establezca el valor del umbral a 10%.

```
setopt DBDIAGPATHFSTH 10
```

DBMEMPERCENT

Utilice esta opción para especificar el porcentaje de memoria del espacio de direcciones virtuales dedicado a procesos del gestor de bases de datos.

Si en el sistema se ejecutan aplicaciones distintas del servidor de IBM Spectrum Protect, asegúrese de que el valor permite la memoria adecuada para que puedan ejecutarse las otras aplicaciones.

Sintaxis

```
>>-DBMEMPERCENT--+-porcentaje-+-----><  
'-AUTO-----'
```

Parámetros

porcentaje

Establezca un valor de 10 a 99.

AUTO

El gestor de bases de datos establece el porcentaje automáticamente en un valor entre el 75 por ciento o el 90 por ciento de la RAM del sistema. El valor predeterminado es AUTO.

Ejemplos

```
dbmempercent 50
```

DBMTCPPORT

La opción DBMTCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del gestor de base de datos espera las peticiones de sesiones de cliente.

El número de puerto especificado debe estar reservado para el uso del gestor de bases de datos.

De forma predeterminada, el servidor IBM Spectrum Protect utiliza IPC (Interprocess Communications) para establecer conexiones para las primeras dos agrupaciones de conexiones, con un máximo de 480 conexiones para cada agrupación. Una vez establecidas las primeras 960 conexiones, el servidor IBM Spectrum Protect utiliza TCP/IP para cualquier conexión adicional.

Sintaxis

```
>>-DBMTCPPort--número_puerto-----><
```

Parámetros

número_puerto

Especifica el número del puerto TCP/IP en el que el servidor de bases de datos espera las comunicaciones del servidor. Los valores válidos son los enteros del 1024 al 65535.

El número de puerto predeterminado es el valor de la opción TCPPORT del servidor más 50.000. Por ejemplo, si la opción TCPPORT del servidor es 1500, el número de puerto de DBMTCPPORT predeterminado sería 51500.

Si la opción de servidor TCPPORT es mayor que 9999, sume los últimos cuatro dígitos de su valor a 50000. Por ejemplo, si la opción TCPPORT es 11500, se suma 1550 a 50000, que da como resultado un número de puerto de DBMTCPPORT de 51500.

Ejemplo

dbmtcport 51500

DEDUPREQUIRESBACKUP

La opción DEDUPREQUIRESBACKUP especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la deduplicación de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.

Si el valor de esta opción es YES (el valor predeterminado), debe realizar la copia de seguridad de los datos en agrupaciones de almacenamiento de copia que no se hayan establecido para la eliminación de datos duplicados. Utilice el mandato BACKUP STGPOOL para efectuar una copia de seguridad de los datos en agrupaciones de almacenamiento de copias.

Tenga en cuenta que es posible que la reclamación de un volumen de una agrupación de almacenamiento establecida para la eliminación de datos duplicados no se produzca cuando el primer volumen puede seleccionarse. El servidor realiza comprobaciones adicionales para asegurarse de que se ha realizado una copia de seguridad de los datos de una agrupación de almacenamiento configurada para la eliminación de los datos duplicados en una agrupación de almacenamiento de copia. Estas comprobaciones requieren más de una instancia de BACKUP STGPOOL antes de que el servidor reclame un volumen. Una vez que el servidor verifica que se ha realizado copia de seguridad de los datos, se reclama el volumen.

Puede cambiar esta opción dinámicamente con el mandato SETOPT.

Atención: Para minimizar la posibilidad de que se produzca una pérdida de datos, no cambie el valor predeterminado de esta opción del servidor. Especifique el valor NO sólo si no tiene ninguna agrupación de almacenamiento de copia y no realiza copias de seguridad de agrupación de almacenamiento.

Sintaxis

```
>>-DEDUPREQUIRESBACKUP--+-Yes+-----<<
                          '-No--'
```

Parámetros

Yes

Especifica que debe realizarse la copia de seguridad de la agrupación de almacenamiento para que los volúmenes puedan reclamarse y para que los datos duplicados puedan descartarse. Este es el valor predeterminado.

No

Especifica que los volúmenes de las agrupaciones de almacenamiento de acceso secuencial primario configuradas para eliminación de datos duplicados se pueden reclamar y si no se realiza una copia de seguridad de las agrupaciones de almacenamiento, los datos duplicados pueden descartarse.

Ejemplos

Especificar que no ha de realizarse la copia de seguridad de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la eliminación de datos duplicados.

```
deduprequiresbackup no
```

DEDUPTIER2FILESIZE

La opción DEDUPTIER2FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 2.

Sintaxis

```
>>-DEDUPTIER2FILESIZE--nnn-----<<
```

Parámetros

nnn

Especifica el tamaño de archivo, en gigabytes, a partir del cual el servidor de IBM Spectrum Protect empieza a utilizar el procesamiento de nivel 2 para la deduplicación de datos. Puede especificar un valor del 20 al 9999. El valor predeterminado es 100.

Nota: Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de la opción SERVERDEDUPTXNLIMIT, esta opción se ignora para la eliminación de datos duplicados del servidor. Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de CLIENTDEDUPTXNLIMIT, esta opción se ignora para la eliminación de duplicados de datos del cliente.

Ejemplos

```
deduptier2filesize 550
```

DEDUPTIER3FILESIZE

La opción DEDUPTIER3FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 3.

Sintaxis

```
>>-DEDUPTIER3FILESIZE--nnn-----<<
```

Parámetros

nnn

Especifica el tamaño de archivo, en gigabytes, a partir del cual el servidor de IBM Spectrum Protect empieza a utilizar el procesamiento de nivel 3 para la deduplicación de datos. Puede especificar un valor del 90 al 9999. El valor predeterminado es 400.

- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de la opción SERVERDEDUPTXNLIMIT, esta opción se ignora para la eliminación de datos duplicados del servidor.
- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de CLIENTDEDUPTXNLIMIT, esta opción se ignora para la eliminación de duplicados de datos del cliente.
- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es menor que el valor especificado o que se ha tomado como valor predeterminado para DEDUPTIER2FILESIZE, el valor de DEDUPTIER2FILESIZE se utiliza para esta opción.

Ejemplos

```
deduptier3filesize 1150
```

DEVCONFIG

La opción DEVCONFIG especifica el nombre de un archivo en el que el usuario quiere que IBM Spectrum Protect almacene una copia de seguridad de la información de configuración del dispositivo.

IBM Spectrum Protect almacena la información siguiente en el archivo de configuración de dispositivos:

- Las definiciones de la clase de dispositivo creadas utilizando el mandato DEFINE DEVCLASS
- Definiciones de unidades creadas utilizando el mandato DEFINE DRIVE
- Definiciones de bibliotecas creadas utilizando el mandato DEFINE LIBRARY
- Información de inventario de biblioteca para las bibliotecas LIBTYPE=SCSI automatizadas
- Las definiciones de vía de acceso creadas utilizando el mandato DEFINE PATH
- Las definiciones de servidor creadas con el mandato DEFINE SERVER
- El nombre del servidor creado con el mandato SET SERVERNAME
- La contraseña del servidor creada con el mandato SET SERVERPASSWORD

Nota:

- Solo se hace una copia de seguridad de las definiciones de vía de acceso con SRCTYPE=SERVER en el archivo de configuración del dispositivo. Las vías de acceso de SRCTYPE=DATAMOVER no se graban en el archivo.
- La información de la ubicación de volúmenes de biblioteca se almacena como comentarios (/!*...*/) en el archivo de configuración de dispositivo siempre que se emitan los mandatos CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME y AUDIT LIBRARY para las

bibliotecas SCSI.

Atención: Para restaurar la base de datos después de un siniestro, debe tener una copia del archivo de configuración del dispositivo actual. El archivo de configuración del dispositivo no se puede volver a crear.

Puede incluir una o varias opciones DEVCONFIG en el archivo de opciones de servidor. Si utiliza varias opciones DEVCONFIG, IBM Spectrum Protect actualiza y almacena automáticamente una copia de seguridad de la información de configuración del dispositivo en cada archivo especificado.

Sintaxis

```
>>-DEVCONFig--nombre_archivo-----><
```

Parámetros

nombre_archivo

Especifica el nombre del archivo en el que debe almacenarse una copia de seguridad de la información de configuración de dispositivos.

Ejemplos

```
devconfig devices.sav
```

DISABLEREORGTABLE

La opción DISABLEREORGTABLE especifica si está inhabilitada la reorganización de tabla para los nombres de tabla especificado en la lista de tablas.

Para utilizar la opción DISABLEREORGTABLE, debe detener el servidor, actualizar el archivo de opciones y, a continuación, reiniciar el servidor.

Sintaxis

```
>>-DISABLEREORGTaBle----tablelist-----><
```

Parámetros

tablelist

Especifica una lista de nombres de tablas para la que está inhabilitada la reorganización de tabla. Si no especifica ningún nombre de tabla con la opción, o si la opción no está en el archivo de opciones, no hay ninguna tabla inhabilitada.

Restricción: Las tablas siguientes ya están excluidas del proceso de reorganización de tabla y no se pueden especificar para esta opción:

- STAGED_EXPIRING_OBJECTS
- STAGED_OBJECT_IDS
- BF_DEREFERENCED_CHUNKS
- BF_QUEUED_CHUNKS

Ejemplo

```
DISABLEREORGTABLE BF_BITFILE_EXTENTS,REPLICATING_OBJECTS
```

DISABLESCHEDS

La opción DISABLESCHEDS especifica si se desactivan las planificaciones de cliente y de administración durante una recuperación del servidor de IBM Spectrum Protect.

Sintaxis

```
>>-DISABLESCheds---+Yes+-----><
```

'-No--'

Parámetros

Yes

Especifica que se desactivan las planificaciones de cliente y de administración.

No

Especifica que se activan las planificaciones de cliente y de administración.

Ejemplos

```
disablescheds no
```

DISPLAYLFINFO

La opción DISPLAYLFINFO especifica el modo en que los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del nodo.

Cuando esta opción está activada, los registros de contabilidad y las entradas de la tabla resumen proporcionarán el valor node_name(storage_agent_name) para el nombre del nodo. Si la opción no está activada, los registros de contabilidad y las entradas de la tabla resumen sólo proporcionarán node_name para el nombre de nodo. El valor predeterminado es No.

Sintaxis

```
>>-DISPLAYLFINFO--+-Yes+-----<<  
      '-No--'
```

Parámetros

Yes

Especifica que los registros de contabilidad y las entradas de la tabla resumen informarán sobre el nombre del agente de almacenamiento

No

Especifica que los registros de contabilidad y las entradas de la tabla resumen no informarán sobre el nombre del agente de almacenamiento. Este es el valor predeterminado.

Ejemplos

```
displaylfinfo yes
```

El resultado muestra el siguiente registro de contabilidad con el nombre de agente de almacenamiento visualizado (STA53):

```
5,0,ADSM,07/13/2004,15:35:14,COLIND-TUC(STA53),,WinNT,1,Tcp/Ip,1,0,0,0,  
0,223,4063,0,0,222,7,8,3,1,4,0,0,0,0,3,0
```

La tabla resumen correspondiente también muestra el nombre del agente de almacenamiento:

```
HORA_INICIO: 2004-07-13 15:35:07.000000  
END_TIME: 2004-07-13 15:35:14.000000  
ACTIVITY: BACKUP  
NUMBER: 8  
ENTITY: COLIND-TUC(STA53)  
COMMETH: Tcp/Ip  
ADDRESS: colind-tuc:2229  
SCHEDULE_NAME:  
EXAMINED: 0  
AFFECTED: 223  
FAILED: 0  
BYTES: 4160875  
IDLE: 8  
MEDIWA: 1  
PROCESSES: 1  
SUCCESSFUL: YES  
VOLUME_NAME:  
DRIVE_NAME:  
LIBRARY_NAME:
```

```
LAST_USE:
COMM_WAIT: 3
NUM_OFFSITE_VOLS:
```

DNSLOOKUP

La opción DNSLOOKUP especifica si el servidor utiliza llamadas de API del sistema para determinar los nombres de servidor de nombres de dominio (DNS) de los sistemas que establecen contacto con el servidor.

Sintaxis

```
>>-DNSLOOKUP--+-Yes+-----<<
      '-No--'
```

Parámetros

Yes

Especifica que el servidor obtiene los nombres DNS de los sistemas que establecen un contacto. El valor predeterminado es Yes.

No

Especifica que el servidor no obtiene los nombres DNS de los sistemas que establecen un contacto.

Ejemplos

```
dnslookup yes
```

DRIVEACQUIRERETRY

La opción DRIVEACQUIRERETRY le permite especificar el número de veces que el servidor reintentará la adquisición de una unidad en una biblioteca IBM® 349x. Si se comparte la biblioteca entre varias aplicaciones, puede parecer que sus unidades están disponibles en el servidor (mediante un proceso subordinado de sondeo), cuando en realidad no lo están.

Esta opción es válida solamente si ha especificado 3494SHARED YES en el archivo de opciones dsmserv.opt. Si ha especificado DRIVEACQUIRERETRY NEVER, debe supervisar el tiempo durante el que los archivos han estado esperando unidades y el tiempo durante el que el servidor ha estado sondeando las unidades. Puede que también tenga que comprobar el estado de estas unidades en los demás servidores de IBM Spectrum Protect. Puede haber cartuchos en las unidades y los demás servidores de IBM Spectrum Protect pueden haber marcado las unidades como *desactivadas*. Si éste es el caso, tendrá que marcar las unidades como *desactivadas* en el servidor de IBM Spectrum Protect que está sondeando las unidades. Si es necesario, cancele también los trabajos en espera.

Sintaxis

```
>>-DRIVEACQuireretry--+-Forever-----+-----<<
      +-Never-----+
      '-número_de_reintentos-'
```

Parámetros

Forever

La adquisición de una unidad se reintenta hasta que se ha adquirido una correctamente. Este es el valor predeterminado.

Never

El servidor no reintenta la adquisición de una unidad y cancela la operación.

número_de_reintentos

Especifica el número máximo de veces, de 1 a 9999, que el servidor reintenta la adquisición de una unidad.

Ejemplos

Especificar que el servidor debe intentar 10 veces como máximo adquirir la unidad.

```
driveacquireretry 10
```

ENABLENASDEDUP

La opción de servidor ENABLENASDEDUP especifica si el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos de almacenamiento conectado a red (NAS). Esta opción solo se aplica a los servidores de archivos NetApp.

Si el valor de la opción es NO, los datos almacenados mediante el servidor de archivos se omiten durante el proceso de identificación de duplicados. Si el valor de esta opción es YES, el valor del parámetro DEDUPLICATE en la definición de agrupación de almacenamiento debe ser YES.

Sintaxis

```
>>-ENABLENASDEDUP---No---+-----<<
      '-Yes-'
```

Parámetros

Yes

Especifique que el servidor de IBM Spectrum Protect optimiza el almacenamiento de los datos almacenados por un servidor de archivos NetApp.

No

Especifica que el servidor no optimiza el almacenamiento de los datos almacenados mediante el servidor de archivos NetApp.

Ejemplo

Especifique que el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos NetApp.

```
enablenasdedup yes
```

EVENTSERVER

La opción EVENTSERVER especifica si, en el momento del arranque, el servidor debe intentar establecer contacto con el servidor de eventos.

Sintaxis

```
>>-EVENTSERVER---Yes---+-----<<
      '-No--'
```

Parámetros

Yes

Especifica que, en el momento del arranque, el servidor intenta establecer contacto con el servidor de eventos. El contacto se establece sólo si ya se ha emitido un mandato DEFINE EVENTSERVER. Este es el valor predeterminado.

No

Especifica que, en el momento del arranque, el servidor no intenta establecer contacto con el servidor de eventos.

Ejemplos

```
eventserver yes
```

EXPINTERVAL

La opción EXPINTERVAL especifica el intervalo, en horas, que ha de transcurrir entre los procesos automáticos de caducidad de inventario que realiza IBM Spectrum Protect. El proceso de caducidad de inventario elimina las copias de seguridad y las copias archivadas del servidor, según se haya especificado mediante las clases de gestión a las que están vinculados los archivos del cliente. Si no se ejecuta periódicamente el proceso de caducidad, no se reclamará el espacio de agrupación de almacenamiento de los archivos del cliente caducados, y el servidor necesitará más espacio de almacenamiento del que necesita según la política.

También puede utilizar el mandato EXPIRE INVENTORY para arrancar manualmente el proceso de caducidad de inventario. El proceso de caducidad puede poner espacio disponible en sus agrupaciones de almacenamiento para copias archivadas o copias de seguridad del cliente adicionales.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
                .-24----.  
>>-EXPINterval--+-horas-+-----<<
```

Parámetros

horas

Especifica el tiempo, en horas, entre procesos automáticos de caducidad de inventario. Puede especificar de 0 a 336 (14 días). El valor 0 significa que el proceso de caducidad debe iniciarse con el mandato EXPIRE INVENTORY. El valor predeterminado es 24.

Ejemplos

```
expinterval 5
```

EXPQUIET

La opción EXPQUIET especifica si IBM Spectrum Protect ha de enviar mensajes detallados durante el proceso de caducidad.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-EXPQUIet--+- --No-+-----<<  
                '- --Sí-'
```

Parámetros

No

Especifica que el servidor envía mensajes detallados. Este es el valor predeterminado.

Yes

Especifica que el servidor sólo envía mensajes mínimos. Estos mensajes se envían únicamente para los archivos que se han caducado según el grupo de copia de la clase de gestión predeterminada o del período de gracia de retención del dominio.

Ejemplos

```
expquiet no
```

 Sistemas operativos Linux

FASPBEGPORT

La opción FASPBEGPORT especifica el número inicial en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

Para definir el rango de números de puerto, especifique las opciones FASPBEGPORT y FASPENDPORT.

Sintaxis

```
                .-15100-----.  
>>-FASPBEGPort--+-número_puerto_inicial-+-----<<
```

Parámetros

número_puerto_inicial

Especifica el número de puerto inicial para las comunicaciones de red que utilizan la tecnología Aspera FASP. El valor predeterminado es 15100.

Solicite al administrador de red que le ayude a definir el rango de números de puerto:

- Si no ha habilitado el protocolo SSL (capa de sockets seguros) para el par de servidores, asegúrese de que los puertos puedan utilizarse para sockets TCP (protocolo de control de transmisiones).
- Asegúrese de que los puertos puedan utilizarse para conexiones UDP (User Datagram Protocol).
- Asegúrese de que los puertos sean compatibles con las reglas de cortafuegos.

Ejemplo

Si las reglas del cortafuegos requieren que los números de puerto sean mayores que 1800, debe especificar un número de puerto mínimo de 1801:

```
faspbegport 1801
```

Referencia relacionada:

FASPENDDPORT

 Sistemas operativos Linux

FASPENDDPORT

La opción FASPENDDPORT especifica el número final en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

Para definir el rango de números de puerto, especifique las opciones FASPBEGPORT y FASPENDDPORT.

Sintaxis

```
.-15199-----  
>>-FASPENDDport--+-número_puerto_final+------<<
```

Parámetros

número_puerto_final

Especifica el número de puerto final para las comunicaciones de red que utilizan la tecnología Aspera FASP. El valor predeterminado es 15199.

Solicite al administrador de red que le ayude a definir el rango de números de puerto:

- Si no ha habilitado el protocolo SSL (capa de sockets seguros) para el par de servidores, asegúrese de que los puertos puedan utilizarse para sockets TCP (protocolo de control de transmisiones).
- Asegúrese de que los puertos puedan utilizarse para conexiones UDP (User Datagram Protocol).
- Asegúrese de que los puertos sean compatibles con las reglas de cortafuegos.


Ejemplo

Si las reglas de cortafuegos requiere números de puerto inferiores a 1900, debería especificar un número de puerto máximo de 1899:

```
faspendport 1899
```

Referencia relacionada:

FASPBEGPORT

 Sistemas operativos Linux

FASPTARGETRATE

La opción FASPTARGETRATE especifica la tasa de destino para la transferencia de datos con la tecnología Aspera Fast Adaptive Secure Protocol (FASP) Si especifica la tasa de destino, limita el ancho de banda de cada conexión de red que utiliza la tecnología Aspera FASP. De este modo, puede asegurarse de que hay suficiente ancho de banda disponible para todas las conexiones de red.

Sintaxis

```
.-250000-----.  
>>-FaspTargetRate---+tasa_destino+----->>
```

Parámetros

tasa_destino

Especifica la tasa máxima, en kilobits por segundo, para la transferencia de datos durante una sesión. El valor predeterminado es 250000. Puede especificar valores en un rango de 100 - 100000000.

Por ejemplo, si emite el mandato PROTECT STGPOOL para ejecutar dos operaciones paralelas en la tasa de destino predeterminado, el rendimiento agregado no supera los 500.000 kbps. Si el sistema de archivos da soporte a dos operaciones para proteger las agrupaciones de datos en tasas mucho más altas que 500.000 kbps de rendimiento agregado, y está disponible el ancho de banda de red suficiente, puede aumentar la tasa de destino.

Para determinar la tasa de destino apropiada, consulte a su administrador de red.

Ejemplos

Si el ancho de banda de red asignado es de 150.000 kbps, puede establecer la tasa de destino en 75.000 y utilizar el número de sesiones predeterminado (dos) para el mandato PROTECT STGPOOL.

```
fasptargetrate 75000
```

En una configuración blueprint de gran tamaño, si el ancho de red asignado es de 6.000,000 kbps, puede establecer la tasa de destino en 750.000 y utilizar ocho sesiones para el mandato PROTECT STGPOOL.

```
fasptargetrate 750000
```

FFDCLOGLEVEL

La opción FFDCLOGLEVEL especifica el tipo de mensajes del servidor generales que se muestran en el registro FFDC (First Failure Data Capture).

El registro FFDC contiene tres categorías de mensajes generales del servidor. Si se establece la opción FFDCLOGLEVEL, las siguientes categorías resultan afectadas:

- FFDC_GENERAL_SERVER_INFO
- FFDC_GENERAL_SERVER_WARNING
- FFDC_GENERAL_SERVER_ERROR

Sintaxis

```
.-FFDCLOGLevel-----ALL-----.  
>>-+FFDCLOGLevel-----+ALL---+----->>  
      +-WARN---+  
      '-ERRor-'
```

Parámetros

ALL

Especifica que todos los mensajes generales FFDC de registro del servidor están en el registro. Este es el valor predeterminado.

WARN

Especifica que aparecen los mensajes FFDC_GENERAL_SERVER_WARNING y FFDC_GENERAL_SERVER_ERROR en el registro.

ERRor

Especifica que solo aparecen los mensajes FFDC_GENERAL_SERVER_ERROR en el registro.

Ejemplo

```
ffdcloglevel warn
```

FFDCLOGNAME

La opción FFDCLOGNAME especifica un nombre del registro FFDC (First Failure Data Capture).

El archivo de registro FFDC se utiliza para recopilar información de diagnóstico sobre el servidor. Cuando ocurre un error, los datos sobre el error se escriben en el archivo de registro FFDC. Esta información se puede proporcionar al soporte de IBM para ayudar a diagnosticar problemas. El archivo de registro FFDC se encuentra en el directorio de la instancia del servidor.

Sintaxis

```
.-dsmffdc.log----.  
>>-FFDCLOGNAME--+-nombre_archivo+-----><
```

Parámetros

nombre_archivo

Especifica un nombre de archivo para el archivo de registro FFDC. El nombre de archivo puede ser un nombre de archivo totalmente calificado o un nombre de archivo relativo al directorio de la instancia del servidor. El valor predeterminado es dsmffdc.log.

Ejemplos

```
ffdclogname /tsminst1/tsmffdc.log  
ffdclogname tsmffdc.log  
ffdclogname c:\tmserv1\tsmffdc.log
```

Referencia relacionada:

FFDCMAXLOGSIZE
FFDCNUMLOGS

FFDCMAXLOGSIZE

La opción FFDCMAXLOGSIZE especifica el tamaño del archivo de registro FFDC (First Failure Data Capture).

El archivo de registro FFDC se utiliza para recopilar información de diagnóstico sobre el servidor. Cuando ocurre un error, los datos sobre el error se escriben en el archivo de registro FFDC. Esta información se puede proporcionar al soporte de IBM para ayudar a diagnosticar problemas.

Sintaxis

```
.-1024-----.  
>>-FFDCMAXLOGSIZE--+-kilobytes+-----><
```

Parámetros

kilobytes

Especifica el tamaño máximo en que puede crecer FFDC antes del reinicio. El valor mínimo es 500. El valor máximo es 2097151. El valor predeterminado es 1024.

Para permitir que el tamaño del archivo de registro crezca indefinidamente, especifique un valor de -1. Para inhabilitar el registro, establezca el valor en -1.

Ejemplos

```
ffdcmaxlogsize 2000
```

Referencia relacionada:

FFDCLOGNAME
FFDCNUMLOGS

FFDCNUMLOGS

La opción FFDCNUMLOGS especifica el número de archivos de registro que se pueden utilizar para el registro circular. El valor predeterminado es 10.

El registro circular utiliza un anillo de archivos de registro para proporcionar recuperación de las anomalías de transacción y de bloqueos del sistema. Por ejemplo, cuando el archivo dsmffdc.log es nulo, se renombra a dsmffdc.log.1. Si el archivo dsmffdc.log.1 existe, el archivo dsmffdc.log.1 se renombra a dsmffdc.log.2. Si existe dsmffdc.log.2, el archivo dsmffdc.log.2 se renombra a dsmffdc.log.3 y así sucesivamente hasta que se alcanza el valor de FFDCNUMLOGS. Si hay un archivo de registro que se renombra como el valor de FFDCNUMLOGS, dicho archivo de registro se suprime.

El valor mínimo es 1. El valor máximo es 100. El valor predeterminado es 10.

Sintaxis

```
.-10----.  
>>-FFDCNUMLOGS---+valor-+-----<<
```

Parámetros

valor

Especifica el número de archivos de registro que se utilizan para el registro circular.

Si especifica el valor 1 y el tamaño del archivo de registro alcanza FFDCMAXLOGSIZE, el servidor continúa escribiendo el archivo de registro. Cualquier información de registro se sobrescribe y el servidor continúa escribiendo el archivo de registro.

Ejemplos

```
ffdcnumlogs 20
```

FILEEXIT

La opción FILEEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es un registro del archivo.

Sintaxis

```
>>-FILEEXIT---+No---+nombre_archivo---+REPLACE---+-----<<  
                '-Yes-'                +-APPEND---+  
                                           '-PRESERVE-'
```

Parámetros

Yes

Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.

No

Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el mandato BEGIN EVENTLOGGING.

nombre_archivo

Especifica el nombre del archivo en el que se han de almacenar los eventos.

REPLACE

Especifica que si existe el archivo, se sobregabará.


APPEND

Especifica que si ya existe un archivo, se agregarán los datos al mismo.

PRESERVE

Especifica que si existe el archivo, no se sobregabará.

Ejemplos

 Sistemas operativos Windows

```
fileexit yes \tsm\server\data replace
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
fileexit yes /tsm/server/data replace
```

FILETEXTEXIT

La opción FILETEXTEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

Sintaxis

```
>>-FILETEXTEXIT--+-No---nombre_archivo---REPLACE-----><
                '-Yes-'                +-APPEND---+
                                           '-PRESERVE-'
```

Parámetros

Yes

Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.

No

Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el mandato BEGIN EVENTLOGGING.

nombre_archivo

Especifica el nombre del archivo en el que se han de almacenar los eventos.

REPLACE

Especifica que si existe el archivo, se sobreguará.


APPEND

Especifica que si existe el archivo, se agregarán los datos al mismo.

PRESERVE

Especifica que si existe el archivo, no se sobreguará.

Ejemplos

 Sistemas operativos Windows

```
filetextexit yes \tsm\server\data replace
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
filetextexit yes /tsm/server/data replace
```

FSUSEDTHRESHOLD

La opción FSUSEDTHRESHOLD especifica qué porcentaje del sistema de archivos puede llenar la base de datos antes emitir un mensaje de alerta.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Si este valor se establece en un número bajo, las anotaciones de actividades pueden inundarse con mensajes que indiquen que el espacio de base de datos se ha llenado, incluso si todavía queda espacio disponible. Si el valor establecido es demasiado alto, el espacio de base de datos puede llenarse antes de poder agregar más espacio al sistema de archivos.

Sintaxis

```
>>-FSUSEDThreshhold--percent-----><
```

Parámetros

porcentaje

Especifica el valor del espacio utilizado en la base de datos. Puede especificar un valor entre 0 y 100. El valor predeterminado es 90.

Ejemplos

```
fsusedthreshold 70
```

IDLETIMEOUT

La opción IDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente puede estar desocupada antes de que la cancele el servidor. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera si existe una gran carga en la red del entorno. Observe, sin embargo, que una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.

La opción de servidor IDLETIMEOUT se utiliza en las sesiones no administrativas. Consulte la opción ADMINIDLETIMEOUT para las sesiones de cliente administrativas.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Sintaxis

```
.-15-----.  
>>-IDLETimeout--+-minutos+-----<<
```

Parámetros

minutos

Especifica el número máximo de minutos que el servidor espera a un cliente desocupado. El valor predeterminado es de 15 minutos. El valor mínimo es de 1 minuto.

Ejemplos

```
idletimeout 15
```

KEEPALIVE

La opción KEEPALIVE especifica si la función keepalive del protocolo de control de transmisiones (TCP) está habilitada para los sockets TCP de salida. La función keepalive TCP envía una transmisión de un dispositivo a otro para comprobar que el enlace entre los dos dispositivos está operativo.

Si está utilizando la réplica de nodo, puede utilizar la opción KEEPALIVE en el servidor de réplica fuente para habilitar la función keepalive de TCP. La opción KEEPALIVE no es necesaria en el servidor de réplica de destino, a menos que especifique la réplica bidireccional, en cuyo caso el servidor de destino se convierte en el servidor de réplica fuente.

Sintaxis

```
.-Yes-.  
>>-KEEPALIVE--+-No+-----<<
```

Parámetros

Yes

Especifica que la función keepalive de TCP está habilitada para los sockets TCP de salida. Este es el valor predeterminado. Si la opción KEEPALIVE está habilitada, se utilizan los valores predeterminados para las opciones KEEPALIVETIME y KEEPALIVEINTERVAL.

No

Especifique que la función keepalive de TCP no está habilitada para los sockets TCP de salida.
Si especifica un valor de NO, no afecta a las conexiones de socket TCP actuales que se han originado de solicitudes de conexión de salida mientras la opción KEEPALIVE estaba establecida en YES. El valor YES se aplica a estos sockets, hasta que la sesión relacionada finalizada y el socket se cierra.

Ejemplo

Utilice el mandato SETOPT para habilitar la función keepalive sin inhabilitar o detener el servidor:

```
setopt keepalive yes
```

Referencia relacionada:

KEEPALIVEINTERVAL
KEEPALIVETIME

KEEPALIVETIME

La opción KEEPALIVETIME especifica la frecuencia con la que TCP envía una transmisión de estado activo cuando recibe una respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.

Sintaxis

```
                .-300-----.  
>>-KEEPALIVETIME--+-segundos-+-----<<
```

Parámetros

seconds

Especifica la frecuencia con la que TCP envía transmisiones de estado activo para verificar que una conexión inactiva sigue activa. El valor se especifica en segundos.

Puede especificar un valor en el rango de 1 a 4294967. El valor predeterminado es 300 (5 minutos).

Ejemplo

Establezca la opción KEEPALIVETIME en 120 segundos:

```
keepalivetime 120
```

Referencia relacionada:

KEEPALIVE
KEEPALIVEINTERVAL

KEEPALIVEINTERVAL

La opción KEEPALIVEINTERVAL especifica la frecuencia con la que se envía una transmisión de estado activo, si no se recibe ninguna respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.

Sintaxis

```
                .-30-----.  
>>-KEEPALIVEINTERVAL--+-segundos-+-----<<
```

Parámetros

seconds

Especifica la longitud de tiempo, en segundos, entre las transmisiones de estado activo, cuando no se recibe ninguna respuesta. El valor se especifica en segundos.

Puede especificar un valor en el rango de 1 a 4294967. El valor predeterminado es 30 segundos.

Ejemplo

Establezca la opción KEEPALIVEINTERVAL en 45 segundos:

```
keepaliveinterval 45
```



Referencia relacionada:


KEEPALIVE
KEEPALIVETIME

LANGUAGE

La opción LANGUAGE controla la inicialización de los entornos nacionales. Un entorno nacional incluye el idioma y los formatos de fecha, hora y número que se han de utilizar para la consola y el servidor.

Si el cliente y el servidor se ejecutan en idiomas diferentes, es posible que los mensajes que se generen puedan ser incomprensibles cuando los mensajes se emiten desde el cliente al servidor o si el servidor envía la salida al cliente.

 Sistemas operativos AIX  Sistemas operativos Linux Si la inicialización del entorno nacional no se ejecuta correctamente, el servidor tomará, de forma predeterminada, el entorno correspondiente al inglés de Estados Unidos.

 Sistemas operativos Windows Si falla la inicialización del entorno nacional, el servidor toma de forma predeterminada el inglés americano y utiliza los formatos de fecha, hora y número que están establecidos mediante las opciones del servidor DATEFORMAT, TIMEFORMAT y NUMBERFORMAT.


Sintaxis


```
>>>-LANGuage--+-AMENG-----><
      |      (2)      |
      +-en_US-----+
      |      (3) |
      '-entorno_local-----'
```

Notas:



1. AMENG sólo está disponible en HP-UX, Solaris, Windows.
2. en_US sólo está disponible en AIX y Linux.
3. *entorno_local* sólo está disponible en AIX, HP-UX, Solaris, Linux y Windows.

Parámetros

 Sistemas operativos Windows AMENG

 Sistemas operativos Windows Especifica que se utilice el inglés americano como idioma predeterminado para el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux en_US

 Sistemas operativos AIX  Sistemas operativos Linux Especifica que se utilice el inglés americano como idioma predeterminado para el servidor.

entorno_local

Especifica el nombre del entorno local al que el servidor da soporte. Consulte las tablas siguientes para obtener información sobre los entornos nacionales soportados por el sistema operativo.

Nota: IBM Spectrum Protect ejecuta cualquier entorno nacional pero el valor predeterminado es inglés de EE.UU. Se dispone de soporte de idiomas para todos los entornos nacionales que figuran en la lista.


 Sistemas operativos AIX

Tabla 1. Idiomas del servidor para AIX

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
Chino, simplificado	Zh_CN
Chino, simplificado (UTF-8)	ZH_CN
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (UTF-8)	ZH_TW
Chino, tradicional (euc_tw)	zh_TW
Inglés	en_US

Idioma	Valor de la opción LANGUAGE
Inglés (UTF-8)	EN_US
Francés	fr_FR
Francés (UTF-8)	FR_FR
Alemán	de_DE
Alemán (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonés, EUC	ja_JP
Japonés, PC	Ja_JP
Japonés, UTF8	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Portugués, de Brasil	pt_BR
Portugués, de Brasil (UTF-8)	PT_BR
Ruso	ru_RU
Ruso (UTF-8)	RU_RU
Español	es_ES
Español (UTF-8)	ES_ES
Nota a pie de tabla: El sistema debe tener instalado el soporte para el entorno en_US.	


 Sistemas operativos Linux

Tabla 2. Idiomas del servidor para Linux

LANGUAGE	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chino, tradicional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Inglés de Estados Unidos	en_US
	en_US.utf8
Francés	fr_FR
	fr_FR.utf8
Alemán	de_DE
	de_DE.utf8
Italiano	it_IT
	it_IT.utf8
Japonés	ja_JP
	ja_JP.utf8
Coreano	ko_KR
	ko_KR.utf8
Portugués, de Brasil	pt_BR
	pt_BR.utf8

LANGUAGE	Valor de la opción LANGUAGE
Ruso	ru_RU
	ru_RU.utf8
Español	es_ES
	es_ES.utf8


 Sistemas operativos Windows


Tabla 3. Idiomas del servidor para Windows

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	chs
Chino, tradicional	cht
Inglés	ameng
Francés	fra
Alemán	deu
Italiano	ita
Japonés	jpn
Coreano	kor
Portugués, de Brasil	ptb
Ruso	rus
Español	esp

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
lang ja_JP
```

 Sistemas operativos Windows

```
lang jpn
```

LDAPCACHEDURATION

La opción LDAPCACHEDURATION determina la cantidad de tiempo que el servidor IBM Spectrum Protect almacena en memoria caché la información de autenticación de contraseña LDAP.

Después de un enlace LDAP satisfactorio, el valor que introduce determina la cantidad de tiempo que la información sobre el servidor de directorios LDAP está disponible. Cuanto mayor sea el número, mejor será el rendimiento del servidor de directorios LDAP. Sin embargo, durante el periodo de caché, los cambios en el servidor de directorios LDAP o tienen efecto inmediato en el nodo. Por ejemplo, puede que las contraseñas antiguas estén disponibles durante algún tiempo, incluso después de que se cambiaran o bloquearan en el servidor LDAP.

Incluya la opción LDAPCACHEDURATION en un mandato SETOPT para que la opción surta efecto inmediatamente.

Restricción: La opción LDAPCACHEDURATION no se aplica a los agentes de almacenamiento.

Sintaxis

```
>>-LDAPCACHEDURATION - minutos----->>
```

Parámetros

minutos

Especifica la cantidad máxima de tiempo después de un enlace LDAP correcto, que las sesiones posteriores para el mismo nodo o administrador se saltan para operaciones de enlace LDAP secundarias. El rango de valores va de cero a 360 minutos.

Ejemplo: establecer el valor LDAPCACHEDURATION a 6 horas (máximo)

En el archivo dmserv.opt , especifique el siguiente valor:

```
ldapcacheduration 360
```

Después de que un nodo o administrador se autentica con un servidor de directorio externo, se salta el enlace LDAP para 360 minutos en todas las sesiones.

LDAPURL

La opción LDAPURL especifica la ubicación de un servidor LDAP (Lightweight Directory Access Protocol). Establezca la opción de LDAPURL después de configurar el servidor LDAP.

Consejo: La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Se aplican las restricciones siguientes:

- La opción LDAPURL no se puede utilizar en combinación con el mandato SETOPT.
- La opción LDAPURL no se aplica a los agentes de almacenamiento.

Sintaxis

```
>>-LDAPURL--ldap_url_value-----<<
```

Parámetros

ldap_url_value

Especifica la dirección URL de un servidor de directorios LDAP, o los URL de varios servidores LDAP. Puede entrar múltiples valores, con cada valor de URL de hasta 1024 caracteres. El número de puerto es opcional y tiene un valor predeterminado de 389. Cada valor de URL debe contener un nombre de servidor LDAP. Por ejemplo, el formato del nombre de servidor es `server1.storage.us.ibm.com` y el puerto LDAP es 341. El valor de la opción LDAPURL debe cumplir las especificaciones siguientes:

- Si especifica varios URL, cada uno debe estar en una línea diferente.
- Si especifica varios URL, cada URL debe apuntar a un directorio externo diferente y todos los directorios externos deben contener los mismos datos.
- Cada URL debe empezar por `ldap://`.
Restricción: La URL que designe no puede comenzar con `ldaps://`.

IBM Spectrum Protect soporta conexiones LDAP aseguradas con una operación LDAPv3 StartTLS estándar que establece un intercambio TLS (Transport Layer Security) en una conexión LDAP existente. La operación LDAP Simple Bind que utiliza IBM Spectrum Protect no protege la contraseña cuando se envía. Se necesita una conexión TLS segura para proteger la contraseña.

Ejemplo: establecer el valor port para un servidor LDAP

En el archivo dmserv.opt , especifique el valor del puerto como 341 para un servidor LDAP:

```
ldapurl ldap://server1.storage.us.ibm.com:341/dc=storage,dc=us,dc=ibm,dc=com
```

MAXSESSIONS

La opción MAXSESSIONS especifica el número máximo de sesiones cliente simultáneas que se pueden conectar con el servidor.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
.-25-----.
```

```
>>-MAXSessions---+número_de_sesiones+-----><
```

Parámetros

número_de_sesiones

Especifica el número máximo de sesiones cliente simultáneas. El valor predeterminado es de 25 sesiones cliente. El valor mínimo es de 2 sesiones clientes. El valor máximo está limitado únicamente por el tamaño de almacenamiento virtual disponible o por los recursos de comunicaciones.

Ejemplos

```
maxsessions 25
```

MESSAGEFORMAT

La opción MESSAGEFORMAT especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.

Sintaxis

```
>>-MESsageformat--número-----><
```

Parámetros

número

Seleccione un número para especificar si se ha de visualizar un número de mensaje únicamente en la primera línea de un mensaje de varias líneas o si se ha de visualizar en todas las líneas.

1

El número del mensaje sólo se visualiza en la primera línea del mensaje. Este es el valor predeterminado.

2

El número del mensaje se visualiza en todas las líneas de un mensaje.

Ejemplos

```
messageformat 2
```

MIRRORLOGDIRECTORY

La opción MIRRORLOGDIRECTORY especifica el directorio para duplicar la vía de acceso de registro activo.

Todos los cambios realizados en el directorio de anotaciones activas también se grabarán en este directorio de duplicación. Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT. Normalmente, no es necesario cambiar el directorio.

Sintaxis

```
>>-MIRRorlogdirectory--dir_name-----><
```

Parámetros

nombre_dir

Especifica un nombre de directorio cualificado al completo para la duplicación de anotaciones activas. El número máximo de caracteres es 175.

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
mirrorlogdirectory /tsm/mirrorlog
```

 Sistemas operativos Windows

MOVEBATCHSIZE

La opción MOVEBATCHSIZE especifica el número de archivos cliente que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Este movimiento de datos es el resultado de las operaciones de restauración y copia de seguridad de agrupaciones de almacenamiento, de migración, reclamación y MOVE DATA. Esta opción funciona con la opción MOVESIZETHRESH.

Sintaxis

```
.-1000-----.  
>>-MOVEBatchsize--+número_de_archivos+-----><
```

Parámetros

número_de_archivos

Especifica un número de archivos entre 1 y 1000. El valor predeterminado es 1000.

Ejemplos

```
movebatchsize 100
```

MOVESIZETHRESH

La opción MOVESIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Cuando se alcance este umbral, no se agregarán más archivos al lote actual, y se arrancará una nueva transacción después de que se haya trasladado el lote actual.

Sintaxis

```
.-4096-----.  
>>-MOVESizethresh--+ megabytes+-----><
```

Parámetros

megabytes

Especifica el número de megabytes como un entero comprendido entre 1 y 32.768. El valor predeterminado es 4096. Esta opción se utiliza con la opción MOVEBATCHSIZE.

Ejemplos

```
movesizethresh 500
```

MSGINTERVAL

La opción MSGINTERVAL especifica el tiempo, en minutos, entre los mensajes que solicitan a un operador que monte una cinta para el servidor.

Sintaxis

```
.-1-----.  
>>-MSGINterval--+minutos+-----><
```

Parámetros

minutos

Especifica el intervalo de tiempo en que el servidor solicita al operador que monte una cinta. El valor predeterminado es de 1 minuto. El valor mínimo es de 1 minuto.

Ejemplos

```
msginterval 2
```

 Sistemas operativos Windows

NAMEDPIPENAME

La opción NAMEDPIPENAME especifica un método de comunicaciones que permite que los procesos se comuniquen entre sí sin tener que saber dónde los procesos del emisor y remitente están ubicados. El nombre actúa como un alias, y conecta los dos procesos independientemente de si están en el mismo sistema o en otros dominios conectados.

Sintaxis

```
>>-NAMEDpipename--nombre-----<<
```

Parámetros

nombre

Especifica el nombre de Named Pipes que debe utilizar el servidor. El protocolo Named Pipes es ideal en el caso de que el cliente y el servidor estén en la misma máquina. No es necesario ningún tipo de software de comunicaciones ni configuración.

Ejemplos

```
namedpipename \\.\PIPE\TSMPIPE
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

NDMPCONNECTIONTIMEOUT

La opción de servidor NDMPCONNECTIONTIMEOUT especifica el tiempo, en horas, que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante las operaciones de restauración NDMP a través de la LAN. Las operaciones de restauración NDMP de sistemas de archivos NAS de gran tamaño puede tener periodos prolongados de inactividad. El valor predeterminado es 6.

Sintaxis

```
.-6-----.  
>>-NDMPCONNECTIONTIMEOUT--horas+-----<<
```

Parámetros

horas

El número de horas que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante una operación NDMP a través de la LAN. El valor predeterminado es 6. El mínimo es de 1 hora. El valor máximo es 48 horas.

Ejemplo

Especifique un tiempo de espera de 10 horas antes de que la conexión NDMP exceda el tiempo de espera.

```
ndmpconnectiontimeout 10
```

NDMPCONTROLPORT

La opción NDMPCONTROLPORT especifica el número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP (Network Data Management Protocol). El servidor de IBM Spectrum Protect no funciona como un servidor de cintas NDMP de uso general.

Sintaxis

```
.-10000-----.  
>>-NDMPControlport--+número_puerto+----->>
```

Parámetros

número_puerto

El número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP. El número de puerto debe oscilar entre 1024 y 32767. El valor predeterminado es 10000.

Ejemplos

```
ndmpcontrolport 9999
```

NDMPENABLEKEEPALIVE

La opción del servidor NDMPENABLEKEEPALIVE especifica si el servidor de IBM Spectrum Protect habilita el mantenimiento en actividad de TCP (Transmission Control Protocol) en las conexiones control NDMP (network data-management protocol) en dispositivos NAS (network-attached storage). El valor predeterminado es NO.

El estado activo TCP se implementa en el soporte de red de un sistema operativo. El estado activo TCP impide que una conexión inactiva, de ejecución larga, se cierre mediante el software de cortafuegos, que detecta y cierra conexiones inactivas.

Restricción: Para evitar errores, no habilite el estado activo TCP en determinados tipos de entornos. Un ejemplo son los entornos en los que no existen cortafuegos entre el servidor de IBM Spectrum Protect y un dispositivo NAS. Otro ejemplo son los entornos con cortafuegos que toleran conexiones inactivas de ejecución larga. La habilitación del estado activo TCP en este tipo de entornos puede hacer que una conexión inactiva se cierre inadvertidamente si el socio de conexión no puede responder temporalmente a paquetes de estado activo TCP.

Sintaxis

```
>>-NDMPENABLEKEEPALIVES--+NO--+----->>  
'-YES-'
```




Parámetros

NO

Inhabilitar el estado activo TCP en todas las conexiones de control NDMP. NO es el valor predeterminado.

YES

Habilitar el estado activo TCP en todas las conexiones de control NDMP. El tiempo de inactividad predeterminado antes de que se envíe el primer paquete de estado activo TCP es de 120 minutos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Para cambiar el tiempo de inactividad, utilice la opción de servidor NDMPKEEPIDLEMINUTES.

Ejemplo

Habilitar el estado activo TCP en todas las conexiones de control NDMP de modo que las conexiones NDMP inactivas no se cierren:

```
ndmpenablekeepalive yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

NDMPKEEPIDLEMINUTES

La opción de servidor NDMPKEEPIDLEMINUTES especifica la cantidad de tiempo, en minutos, antes de que el sistema operativo transmita el primer paquete de estado activo TCP (Transmission Control Protocol) en una conexión de control NDMP (Network Data-Management Protocol). El valor predeterminado son 120 minutos.

Requisito previo: Utilice esta opción sólo después de establecer el valor de la opción de servidor NDMPENABLEKEEPALIVES en YES.

Sintaxis

```
.-120-----.  
>>-NDMPKEEPIDLEMINUTES--+-minutes-+-----><
```

Parámetros

minutos

El número de minutos de inactividad en conexiones de control NDMP antes de que se transmitan paquetes de estado activo TCP. El valor predeterminado es 120. El mínimo es 1 minuto. El máximo es de 600 minutos.

Ejemplo

Especificar un tiempo de inactividad de 15 minutos antes de que se envíe el primer paquete de estado activo TCP:

```
ndmpkeepidleminutes 15
```

NDMPPORTRANGE

La opción NDMPPORTRANGE especifica el rango de números de puerto por los que IBM Spectrum Protect pasa en secuencia para obtener un número de puerto para aceptar una sesión de un dispositivo NAS (almacenamiento conectado a red) para la transferencia de datos. El valor predeterminado es 0,0, que significa que IBM Spectrum Protect deja que el sistema operativo proporcione un puerto (puerto efímero).

Si todos los puertos especificados están en uso cuando un dispositivo NAS intenta conectarse con el servidor, la operación no se ejecuta correctamente. Si se selecciona un único número de puerto (sin comas y sin ningún número de puerto para el valor alto), el valor predeterminado para el número de puerto alto es el número de puerto bajo más 100).

Cuando los datos NDMP (Network Data Management Protocol) se dirigen a una agrupación nativa de IBM Spectrum Protect, la comunicación puede iniciarse desde los sistemas NDMP o desde el servidor de IBM Spectrum Protect. Si existe un cortafuegos que separa el servidor y los dispositivos NAS, puede que sea necesario especificar números de puerto en las reglas del cortafuegos para permitir que fluya tráfico hasta y desde los dispositivos NAS. Los dispositivos NAS comunican al servidor de IBM Spectrum Protect los números de puerto que se utilizarán cuando se establezca contacto con el servidor. Los números de puerto del servidor se controlan con las opciones NDMPPortrange. El control del número de puerto para los dispositivos NAS es específico de los proveedores. Consulte la documentación del proveedor.

Sintaxis

```
>>-NDMPPortrange--número_puerto_bajo+-----+----><  
'-,número_puerto_alto-'
```

Parámetros

número_puerto_bajo

El número de puerto bajo desde el que IBM Spectrum Protect inicia el ciclo cuando necesita un número de puerto para aceptar una sesión de un dispositivo NAS para la transferencia de datos. El valor mínimo del número de puerto es 1024.

número_puerto_alto

El número de puerto alto hasta el que puede llegar IBM Spectrum Protect cuando necesita un número para aceptar una sesión de un dispositivo NAS para la transferencia de datos. El valor máximo del número de puerto es 32767. El número de puerto alto debe ser el mismo o más grande que el número de puerto bajo.

Ejemplos

Especifique que IBM Spectrum Protect puede pasar por los números de puerto 1024 a 2024.

```
ndmpportrange 1024,2024
```

NDMPPREFDATAINTERFACE

Esta opción especifica la dirección IP que se asocia a la interfaz en la que desea que el servidor reciba todos los datos de copia de seguridad NDMP (Network Data Management Protocol).

Esta opción afectará a todas las operaciones de archivador a servidor NDMP posteriores, pero no afectará a las conexiones de control NDMP, que utilizan la interfaz de red predeterminada del sistema. El valor de esta opción es un nombre de host o una dirección IPV4 que se asocia a una de las interfaces de red activas del sistema en el que se ejecuta el servidor de IBM Spectrum Protect. Esta interfaz debe haberse activado para IPV4.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Sintaxis

```
>>-NDMPPREFDATAINTERFACE--dirección_ip-----><
```

Parámetros

dirección_ip

Especifique una dirección en formato decimal con puntos o en formato de nombre de host. Si especifica una dirección decimal con puntos, ésta no se verificará con un servidor de nombres de dominio. Si la dirección no es correcta, puede que se produzcan errores cuando el servidor intente abrir un socket durante el inicio de una copia de seguridad de archivador a servidor NDMP.

Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. No existe un valor predeterminado. Si no se establece ningún valor, todas las operaciones NDMP utilizan la interfaz de red del servidor de IBM Spectrum Protect para recibir los datos de copia de seguridad durante las operaciones de copia de seguridad de archivador a servidor NDMP.

Para borrar el valor de la opción, especifique el mandato SETOPT con un valor nulo, "".

Ejemplos:

```
ndmpprefdatainterface net1.tucson.ibm.com
```

```
ndmpprefdatainterface 9.11.152.89
```

NOPREEMPT

El servidor permite que determinadas operaciones tengan prioridad sobre otras operaciones para acceder a volúmenes y dispositivos. Puede especificar la opción NOPREEMPT para desactivar la prioridad. Cuando se desactiva la prioridad, ninguna operación puede tener prioridad sobre otra para acceder a un volumen, y únicamente una operación de copia de seguridad de base de datos puede tener prioridad sobre otra operación para acceder a un dispositivo.

Por ejemplo, una operación de restauración de datos de cliente tiene prioridad sobre una operación de copia de seguridad de datos cliente para utilizar un dispositivo específico o para acceder a un volumen específico.

Sintaxis

```
>>-NOPREEMPT-----><
```

Parámetros

Ninguno

Ejemplos

No permitir que ninguna operación del servidor se adelante a otra:

```
nopreempt
```

NORETRIEVEDATE

La opción NORETRIEVEDATE especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo. Esta opción y el parámetro MIGDELAY de agrupación de almacenamiento controlan cuándo el servidor migra los archivos.

Si no se especifica NORETRIEVEDATE, el servidor migra los archivos una vez han estado en la agrupación de almacenamiento el número de días que especifica el parámetro MIGDELAY. El número de días se cuenta a partir del día en que el archivo se almacenó en la agrupación de almacenamiento o un cliente lo recuperó, lo que sea más reciente. Si especifica NORETRIEVEDATE, el servidor no actualiza la fecha de recuperación de un archivo ni el número de días contados a partir del día en que el archivo entró en la agrupación de almacenamiento en disco.

Si se especifica esta opción y está activada la función de caché para una agrupación de almacenamiento de disco, las operaciones de reclamación de espacio en caché resultarán afectadas. Cuando se necesita espacio en una agrupación de almacenamiento de disco que contiene archivos en caché, el servidor obtiene el espacio borrando las copias en caché de forma selectiva. Los archivos que tienen las fechas de recuperación más antiguas y que ocupan la mayor cantidad de espacio son los que se seleccionan para suprimirlos. Cuando se especifica NORETRIEVEDATE, el servidor no actualiza la fecha de recuperación cuando se recupera un archivo. Esto puede ocasionar que se supriman las copias en caché aunque un cliente las haya recuperado recientemente.

Sintaxis

```
>>-NORETRIEVEDATE-----<<
```

Parámetros

Ninguno.

Ejemplos

Especificar que no se actualizan las fechas de recuperación de los archivos en las agrupaciones de almacenamiento en disco cuando los clientes restauran y recuperan archivos:

```
noretrievevdate
```

 Sistemas operativos Windows

NPAUDITFAILURE

La opción NPAUDITFAILURE especifica si ha de enviarse un evento a las anotaciones de eventos cuando un nodo se conecte con el servidor utilizando un nombre que se encuentra en el grupo de Windows pero que no coincide con el nombre de inicio de sesión de cuenta de Windows. Para garantizar que un nodo pueda acceder sólo a sus propios datos, el nombre del nodo y el nombre de cuenta Windows deben coincidir.

Sintaxis

```
>>-NPAUDITFailure---Yes+-----<<  
      '-No--'
```

Parámetros

Yes

Especifica que un evento se envía a las anotaciones de eventos cuando un nodo inicia una sesión en el servidor con un nombre que forma parte del grupo Windows. Sin embargo, este nombre no coincide con el nombre de inicio de sesión de la cuenta Windows con el que ha iniciado la sesión.


No

Especifica que no se enviará un evento de anomalía de auditoría a las anotaciones de eventos.

Ejemplos

Especifique que se envíe un evento a las anotaciones de eventos cuando un nodo inicie una sesión en el servidor con un nombre que forme parte del grupo Windows. Sin embargo, este nombre no coincide con el nombre de inicio de sesión de la cuenta Windows con el que ha iniciado la sesión.

```
npauditfailure yes
```

 Sistemas operativos Windows

NPAUDITSUCCESS

La opción NPAUDITSUCCESS especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.

Sintaxis

```
>>-NPAUDITSUCCESS--+-Yes+-----<<
                    '-No--'
```

Parámetros

Yes

Especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPES.

No

Especifica que no se envía un evento a las anotaciones de Windows.

Ejemplos

Especificar que se envía un evento a las anotaciones de eventos cuando se autentica un nodo cliente para acceder al servidor.

```
npauditsuccess yes
```

 Sistemas operativos Windows

NPBUFFERSIZE

La opción NPBUFFERSIZE especifica el tamaño del búfer de comunicaciones de Named Pipes.

Sintaxis

```
                    .-8-----.
>>-NPBUFFERSIZE--+-kilobytes+-----<<
```

Parámetros

kilobytes

Especifica el tamaño, en kilobytes, del búfer de comunicaciones de Named Pipes. El valor predeterminado es 8.

Ejemplos

Especificar un búfer de comunicaciones de Named Pipes de 16 KB:

```
npbuffersize 16
```

 Sistemas operativos Windows

NUMBERFORMAT

La opción NUMBERFORMAT especifica el formato de numeración que el servidor utiliza para visualizar los números.

El valor de NUMBERFORMAT se altera temporalmente mediante la definición de formato numérico del entorno nacional si el entorno nacional se inicializa correctamente durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

Sintaxis

```
>>-NUMBERFORMAT--número-----<<
```

Parámetros

número

Seleccione un número de 1 a 6 para identificar el formato de números que utiliza el servidor. El valor predeterminado es 1.

1	1,000.00
2	1,000,00
3	1 000,00
4	1 000.00
5	1.000,00
6	1'000,00

Ejemplos

```
numberformat 4
```

NUMOPENVOLSALLOWED

La opción NUMOPENVOLSALLOWED especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.

Los volúmenes de entrada contienen datos que se deben leer durante operaciones de restauración de cliente y procesos de servidor, como reclamación y migración. Utilice esta opción para mejorar el rendimiento al reducir la frecuencia con la que se abren y cierran los volúmenes.

Cada sesión de un proceso de servidor u operación de cliente puede tener tantos volúmenes FILE como se especifiquen en esta opción. Una sesión la inicia una operación de cliente o un proceso de servidor. Se pueden iniciar varias sesiones en cada uno de ellos.

Durante una operación de restauración de cliente, los volúmenes permanecerán abiertos durante la duración de una operación de restauración de cliente y mientras una sesión de cliente esté activa. Durante una operación de restauración sin consulta, los volúmenes permanecerán abiertos hasta que se complete la restauración sin consulta. En ese momento, se cerrarán todos los volúmenes. Sin embargo, para operaciones de restauración clásicas iniciadas en modalidad interactiva, los volúmenes permanecerán abiertos al final de la operación de restauración. Los volúmenes se cerrarán y liberarán cuando se solicite la próxima operación de restauración clásica.

Establezca este valor en el archivo de opciones del servidor o utilice el mandato SETOPT.

Consejo: Esta opción puede aumentar significativamente el número de volúmenes y puntos de montaje en uso en cualquier momento. Para optimizar el rendimiento, siga estos pasos:

- Para establecer NUMOPENVOLSALLOWED, seleccione un valor de inicio (se recomienda el valor predeterminado). Supervise las sesiones de cliente y los procesos de servidor. Tenga en cuenta el número más alto de volúmenes abiertos para una única sesión o un único proceso. Aumente el valor de NUMOPENVOLSALLOWED si el número más alto de volúmenes abiertos es igual al valor especificado en NUMOPENVOLSALLOWED.
- Para evitar que las sesiones o los procesos tengan que esperar un punto de montaje, aumente el valor del parámetro MOUNTLIMIT en la definición de clase de dispositivo. Establezca el parámetro MOUNTLIMIT en un valor que sea lo suficientemente alto para que permita que todas las sesiones de cliente y todos los procesos de servidor que utilizan agrupaciones de almacenamiento con eliminación de duplicados abran el número de volumen especificado en la opción NUMOPENVOLSALLOWED. Para sesiones de cliente, compruebe el destino en la definición de grupo de copia para determinar cuántos nodos almacenan datos en la agrupación de datos con eliminación de duplicados. Para procesos de servidor, compruebe el número de procesos permitidos para cada proceso para la agrupación de almacenamiento.
- Puede producirse una situación en la que un nodo realice una copia de seguridad y restaure o archive y recupere al mismo tiempo en y desde una agrupación de almacenamiento deduplicada. Todos los puntos de montaje necesarios para estas operaciones aumentan el número total de puntos de montaje necesarios para el nodo.

Como consecuencia, es posible que el nodo no pueda iniciar sesiones de copia de seguridad adicionales si ya tiene más puntos de montaje abiertos de los que permite el parámetro MAXNUMMP de la definición del nodo de cliente. Esto puede suceder aunque el MOUNTLIMIT de la clase de dispositivo no se hubiera excedido.

Para, evitar que las operaciones de copia de seguridad y recuperación fallen, establezca el parámetro MAXNUMMP de la definición de nodo cliente en un valor que sea como mínimo igual de alto que la opción NUMOPENVOLSALLOWED. Aumente este valor si nota que el nodo no está realizando satisfactoriamente operaciones de copia de seguridad o recuperación porque se ha sobrepasado el valor de MAXNUMMP.

Sintaxis

```
>>-NUMOPENVOLSallowed--número_volúmenes_abiertos-----><
```

Parámetros




número_volúmenes_abiertos

Especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado. El valor predeterminado es 10. El valor mínimo es 3 y el máximo es 999.

Ejemplos

Especifique que hasta 5 volúmenes pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.

```
numopenvolsallowed 5
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

PUSHSTATUS

La opción PUSHSTATUS se utiliza en servidores de radio para asegurarse de que la información de estado se envía al servidor concentrador. No actualice esta opción a menos que deba restaurar la configuración del Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o de radio.

Si debe restaurar la configuración del Centro de operaciones al estado preconfigurado, debe emitir el mandato siguiente en cada servidor de radio:

```
SETOPT PUSHSTATUS NO
```

QUERYAUTH

La opción QUERYAUTH especifica el nivel de autorización de administración necesario para emitir los mandatos QUERY o SQL SELECT. De forma predeterminada, cualquier administrador puede emitir los mandatos QUERY y SELECT. Puede utilizar esta opción para restringir el uso de estos mandatos.

Sintaxis

```
>>-QUERYAuth--+-None-----+-----><
+-System---+
+-Policy---+
+-Storage---+
'-Operator-'
```

Parámetros

NOne

Cualquier administrador puede emitir los mandatos QUERY o SELECT sin que sea necesaria ninguna autorización de administración.

System

Los administradores deben tener autorización SYSTEM para emitir los mandatos QUERY o SELECT.

Policy

Los administradores deben tener autorización POLICY sobre uno o varios dominios de políticas, o bien autorización SYSTEM para emitir los mandatos QUERY o SELECT.

Storage

Los administradores deben tener autorización STORAGE sobre una o varias agrupaciones de almacenamiento, o bien autorización SYSTEM para emitir los mandatos QUERY o SELECT.

Operator

Los administradores deben tener autorización OPERATOR o SYSTEM para emitir los mandatos QUERY o SELECT.

Ejemplos

Para restringir el uso de los mandatos QUERY y SELECT a los administradores con autorización de sistema o almacenamiento, especifique lo siguiente:

```
queryauth storage
```

RECLAIMDELAY

Esta opción retrasa la reclamación de un volumen SnapLock y permite que los datos restantes caduquen para que no haya necesidad de reclamar el volumen.

Sintaxis

```
.-4-----.  
>>-RECLAIMDELAY--+-número_de_días-+-----><
```

Parámetros

número_de_días

Especifica el número de días de retraso de la reclamación de un volumen SnapLock.

Antes de reclamar un volumen SnapLock, el servidor de IBM Spectrum Protect permite que transcurra el número de días especificado para que los archivos que queden en el volumen tengan la oportunidad de caducar. El periodo de retraso de reclamación predeterminado es de cuatro días, y los valores posibles son de 1 a 120 días.

Ejemplos

Especifique que el número de días de retraso de la reclamación sea de 30 días:

```
reclaimdelay 30
```

RECLAIMPERIOD

Esta opción permite definir el número de días para el periodo de reclamación de un volumen SnapLock.

Sintaxis

```
.-30-----.  
>>-RECLAIMPERIOD--+-número_de_días-+-----><
```

Parámetros

número_de_días

Especifica el número de días que se permiten para el periodo de reclamación de un volumen SnapLock.

Después de que caduque la retención de un volumen SnapLock, el servidor de IBM Spectrum Protect reclamará el volumen antes de que transcurra el número de días especificado si todavía quedan datos en el volumen. El periodo de reclamación predeterminado es de 30 días y puede establecerse en cualquier lugar y desde 7 a 365 días.

El periodo de reclamación no empieza hasta que ha caducado el periodo RECLAIMDELAY.

Ejemplos

Especificar que el periodo de reclamación sea de 45 días:

```
reclaimperiod 45
```


REORGBEGINTIME

La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o índice.

Planifique las reorganizaciones iniciadas por el servidor para que se inicien durante los periodos en los que la actividad del servidor es baja. Utilice esta opción conjuntamente con la opción REORGDURATION. REORGDURATION especifica un intervalo en el que puede empezar la reorganización.

Sintaxis

```
>>-REORGBEGINTime--hh:mm-----<<
```

Parámetros

hh:mm

Especifica la hora a la que el servidor puede iniciar una reorganización. La hora de inicio predeterminada es a las 6:00. Utilice un formato de 24 horas para especificar la hora.

Hora	Descripción	Valores
hh	La hora del día	Especifique un número de 1 a 23.
mm	El minuto de la hora	Especifique un número de 1 a 59.

Ejemplos

Especificar las 6:00 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 06:00
```

Especificar las 20:30 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 20:30
```

Especificar el mediodía como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 12:00
```

Especificar las 15:30 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 15:30
```

Especificar la medianoche como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 00:00
```

REORGDURATION

La opción REORGDURATION especifica un intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.

Planifique las reorganizaciones iniciadas por el servidor para que se inicien durante los periodos en los que la actividad del servidor es baja. Utilice esta opción conjuntamente con la opción REORGBEGINTIME. La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor puede iniciar una reorganización.

Sintaxis

```
>>-REORGDURation--nn-----<<
```

Parámetros

nn

Especifica el número de horas en las que puede iniciarse una reorganización. El valor mínimo es 1 y el máximo es 24. El valor predeterminado es 24.

Ejemplo

Especifique un intervalo de cuatro horas en las que puede iniciarse una reorganización.

```
reorgduration 4
```

REPORTRETRIEVE

La opción REPORTRETRIEVE genera informes sobre las operaciones de restauración o recuperación que realizan los nodos clientes o los administradores. El valor predeterminado es NO.

Sintaxis

```
>>-REPORTRETRIEVE---YES+-----<<
      '-NO--'
```

Parámetros

YES

Especifica que se emitirán mensajes en la consola del servidor y se almacenarán en las anotaciones de actividad cuando se restauren o recuperen los archivos desde el servidor de IBM Spectrum Protect. Los mensajes especificarán el nombre de los objetos que se están restaurando o recuperando e identificarán el nodo cliente o administrador que realice la operación.

NO

Especifica que no se emitirán mensajes.

Ejemplos

Especificar que han de emitirse y almacenarse mensajes en las anotaciones de actividades siempre que se restauren o recuperen archivos desde el servidor de IBM Spectrum Protect:

```
reportretrieve yes
```

Se emite el siguiente mensaje para una sesión de cliente de administración:

```
ANR0411I Sesión 8 para el administrador COLIND-TUC iniciado como el nodo
COLIND-TUC objeto de copia de seguridad restaurado o recuperado: nodo
COLIND-TUC,
espacio de archivos \\colind-tuc\c$,
object\CODE\TESTDATA\ XXX.OUT
```

REPLBATCHSIZE

La opción REPLBATCHSIZE especifica el número de archivos de cliente que se van a replicar en proceso por lotes, dentro de la misma transacción de servidor. Esta opción afecta únicamente a los procesos de réplica de nodo y funciona con la opción REPLSIZETHRESH para mejorar el proceso de réplica de nodo.

La opción REPLBATCHSIZE limita el número de ficheros en una transacción y la opción REPLSIZETHRESH limita el número de bytes en una transacción. La transacción finaliza cuando se alcanza el umbral de REPLBATCHSIZE o REPLSIZETHRESH.

Sintaxis

```
.-4096-----
>>-REPLBatchsize---number_of_files+-----<<
```

Parámetros

número_de_archivos

Especifica un número de archivos entre 1 y 32768. El valor predeterminado es 4096.

Ejemplos

```
replbatchsize 25000
```

REPLSIZETHRESH

La opción REPLSIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos replicados, dentro de la misma transacción del servidor.

La cantidad de datos se basa en el tamaño del archivo sin eliminación de duplicados, que es el tamaño original del archivo. La cantidad de datos que se replican está controlada por el umbral. Cuando la cantidad de datos supera el umbral, el servidor finaliza la transacción y no se agregan más archivos al lote actual. Se inicia una nueva transacción después de que se replica el lote actual. Esta opción se utiliza con la opción REPLBATCHSIZE.

Por ejemplo, supongamos que un archivo es de 10 MB y se almacena en una agrupación de almacenamiento que tiene habilitada la eliminación de duplicados de datos y sólo 2 MB del archivo se transfiere durante la réplica. La cantidad de datos replicados incluye el tamaño de 10 MB de archivo y excluye los 2 MB transferidos. Cuando la cantidad de datos duplicados supera el valor especificado para el umbral REPLSIZETHRESH, la transacción finaliza.

Consejo: Si está replicando datos desde un servidor de origen en la nube y recibe con frecuencia el mensaje de servidor ANR1880W en el servidor de destino, reduzca el valor de la opción REPLSIZETHRESH en el servidor de origen.

Sintaxis

```
                .-4096-----.  
>>-REPLSizethresh---+ megabytes+-----<<
```

Parámetros

megabytes

Especifica el número de megabytes como un entero comprendido entre 1 y 32.768. El valor predeterminado es 4096.

Ejemplos

```
replsizethresh 2000
```

REQSYSAUTHOUTFILE

La opción REQSYSAUTHOUTFILE especifica si es necesaria la autorización del sistema para los mandatos de administración que hacen que IBM Spectrum Protect realice una grabación en un archivo externo.

Esta opción se puede utilizar con los mandatos siguientes:

- BACKUP DEVCONFIG con el parámetro FILENAMES
- BACKUP VOLHISTORY con el parámetro FILENAMES
- DEFINE BACKUPSET
- DELETE BACKUPSET
- GENERATE BACKUPSET
- MOVE DRMEDIA con el parámetro CMD
- MOVE MEDIA con el parámetro CMD
- QUERY DRMEDIA con el parámetro CMD
- QUERY MEDIA con el parámetro CMD
- QUERY SCRIPT con el parámetro OUTPUTFILE

Sintaxis

```
>>-REQSYSauthoutfile---+Yes+-----<<  
                        '-No--'
```

Parámetros

Yes

Especifica que es necesaria la autorización del sistema para los mandatos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo.

No

Especifica que no es necesaria la autorización del sistema para los mandatos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo. Es decir, no hay ningún cambio en el nivel de autorización necesario para emitir el mandato.

Ejemplos

```
reqsysauthoutfile no
```

RESOURCETIMEOUT

La opción RESOURCETIMEOUT especifica el intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso. Cuando se exceda el tiempo de espera, la petición del recurso se cancelará.

Nota: Al gestionar un conjunto de recursos de bibliotecas compartidos, como servidores designados como gestores y clientes de bibliotecas, plantéese la posibilidad de establecer esta opción en el mismo límite de tiempo para todos los participantes de la configuración compartida. En caso de recuperación de errores, IBM Spectrum Protect siempre aplazará la acción al límite de tiempo más largo.

Sintaxis

```
.-60-----.  
>>-RESOURCETIMEout--+-minutos+-----<<
```

Parámetros

minutos

Especifica el número máximo de minutos que el servidor espera un recurso. El valor predeterminado es de 60 minutos. El valor mínimo es de 1 minuto.

Ejemplos

Especifica que el servidor esperará un recurso de servidor durante 15 minutos:

```
resourcetimeout 15
```

RESTHTTSPORT

La opción RESTHTTSPORT especifica el número de puerto que se utilizará para la comunicación mediante el Protocolo seguro de transferencia de hipertexto (HTTPS) entre el Centro de operaciones y el servidor concentrador.

Sintaxis

```
.-8443-----.  
>>-RESTHTTSPORT--+-puerto_seguro+-----<<
```

Parámetros

puerto_seguro

Especifica el número de puerto que se utiliza para comunicaciones seguras entre el servidor concentrador y el Centro de operaciones. El rango de valores es 1025-32767; el valor predeterminado es 8443.

Ejemplo

Especifica que el número de puerto 8444 se utiliza para la comunicación HTTPS.

```
resthttpsport 8444
```

RESTOREINTERVAL

La opción RESTOREINTERVAL especifica durante cuánto tiempo se puede guardar una sesión de restauración rearrancable en la base de datos del servidor. Siempre y cuando la sesión de restauración se haya guardado en la base de datos, se puede volver a arrancar desde el punto en el que se ha detenido.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
.-1440----.  
>>-RESTOREINTERVAL--+-minutos-+-----><
```

Parámetros

minutos

Especifica el intervalo, en minutos, durante el cual una sesión de restauración rearrancable puede residir en la base de datos del servidor antes de que caduque. El valor mínimo es 0. El valor máximo es 10080 (una semana). El valor predeterminado es de 1440 minutos (24 horas). Si el valor se establece en 0 y la restauración se interrumpe o resulta anómala, de todos modos la restauración se continúa poniendo en estado rearrancable. Sin embargo, queda inmediatamente elegible para su caducidad.

Ejemplos

```
restoreinterval 1440
```

RETENTIONEXTENSION

La opción RETENTIONEXTENSION especifica el número de días que ha de ampliarse la fecha de retención de un volumen de SnapLock. Esta opción permite que el servidor amplíe la fecha de retención de un volumen de SnapLock para evitar las reclamaciones excesivas.

Sintaxis

```
>>-RETENTIONEXTENSION--número_de_días-----><
```

Parámetros

número_de_días

Especifica el número de días para ampliar la fecha de retención de un volumen de SnapLock. El valor mínimo es 30 días; el valor máximo es 9999 días; el valor predeterminado es 365.

Si especifica un valor de 0 (cero) en el parámetro RETVER de un grupo de copia archivada, el valor real que se utiliza para RETVER es el valor de la opción RETENTIONEXTENSION, si se da una de las siguientes condiciones:

- La agrupación de almacenamiento de destino del grupo de copia archivada es una agrupación de almacenamiento SnapLock.
- La agrupación de almacenamiento de destino de una migración de agrupación de almacenamiento o de un mandato MOVE DATA o MOVE NODEDATA es una agrupación de almacenamiento SnapLock.

Si un volumen de SnapLock constituye el volumen de destino de los datos procedentes de otro volumen de SnapLock, y si la retención restante de los datos del volumen es menor que el valor especificado, la fecha de retención se definirá utilizando el valor especificado. De lo contrario, se utilizará la retención restante de los datos para definir la retención del volumen.

Si un volumen de SnapLock ha introducido el período de reclamación pero el porcentaje del espacio reclamable del volumen no ha sobrepasado el umbral de reclamación de la agrupación de almacenamiento o bien el valor especificado en el parámetro THRESHOLD de un mandato RECLAIM STGPOOL, la fecha de retención del volumen de SnapLock se ampliará en función del valor especificado en la opción RETENTIONEXTENSION.

Ejemplos

Especificar que la fecha de retención se amplía en 60 días:

SANDISCOVERY

La opción SANDISCOVERY especifica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.

Para utilizar el descubrimiento de SAN, todos los dispositivos de la SAN deben tener un número de serie de dispositivo exclusivo. Cuando se establece en ON, el servidor realiza el descubrimiento de SAN en las siguientes instancias:

- Cuando se ha cambiado la ruta de acceso del dispositivo
- Cuando se ha emitido el mandato QUERY SAN

Utilizando el descubrimiento de SAN, el servidor puede corregir automáticamente el nombre de archivo especial de un dispositivo si éste se ha cambiado para un dispositivo de cinta especificado.

El servidor de IBM Spectrum Protect no requiere un enlace permanente con la función de descubrimiento de SAN activada. Para mostrar una lista de los dispositivos detectados por el servidor, emita el mandato QUERY SAN.

Sintaxis

```
.-SANDISCOVERY-----OFF-----
>>+-----+----->>
'-SANDISCOVERY-----+ON-----'
          '-UNSCANNEDPATHOFF-'
```

Parámetros

ON

Especifica que el servidor realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el mandato QUERY SAN.

OFF

Especifica que el servidor no realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el mandato QUERY SAN. Si el servidor de IBM Spectrum Protect no puede abrir un dispositivo, se emite un mensaje pero la ruta asociada con el dispositivo no se pone fuera de línea. Este es el valor predeterminado.

UNSCANNEDPATHOFF

Especifica que el servidor no realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el mandato QUERY SAN. Si el servidor de IBM Spectrum Protect no puede abrir un dispositivo, se emite un mensaje y la ruta al dispositivo se pone fuera de línea.




Ejemplos

```
sandiscovery on
```

Mandatos relacionados

Tabla 1. Mandatos relacionados con SANDISCOVERY

Mandato	Descripción
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Windows

SANDISCOVERYTIMEOUT

La opción SANDISCOVERYTIMEOUT especifica la cantidad de tiempo permitido para que respondan los adaptadores de bus de host si se consultan mediante el proceso de descubrimiento de SAN. Cuando se alcance el tiempo especificado en SANDISCOVERYTIMEOUT, el proceso excede el tiempo de espera.

Sintaxis

```
>>-SANDISCOVERYTIMEOUT--valor----->>
```


Parámetros

valor

Especifica la cantidad de tiempo que transcurre antes de que el proceso de descubrimiento de SAN exceda el tiempo de espera. El rango es de 15 a 1800 segundos. El valor predeterminado son 15 segundos.

Ejemplos

```
sandiscoverytimeout 45
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

SANREFRESHTIME

La opción SANREFRESHTIME especifica la cantidad de tiempo que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. La opción SANREFRESHTIME tiene un valor predeterminado de 0, que significa que no hay caché de descubrimiento de SAN. La información se obtiene directamente del adaptador de bus de host (HBA) cada vez que el servidor ejecuta una operación de descubrimiento de SAN.

Nota: El mandato de servidor QUERY SAN siempre recibe información de la SAN en el momento de emitirse el mandato y pasa por alto los valores que se han especificado para SANREFRESHTIME.

Sintaxis

```
.-0----.  
>>-SANREFRESHTIME--+-hora+-----<<
```

Parámetros

hora

Cantidad de tiempo, en segundos, que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. El valor predeterminado es 0 y especifica que la información de descubrimiento de SAN no se guarda en la memoria caché. Si se especifica un valor que no sea 0, como por ejemplo 100 segundos, la información de descubrimiento de SAN se renueva 100 segundos después de la operación de descubrimiento de SAN anterior.

Ejemplos

Renovar la información de descubrimiento de SAN transcurridos 100 segundos.

```
sanrefreshtime 100
```

Desactivar la colocación en caché de la información de descubrimiento de SAN.

```
sanrefreshtime 0
```

SEARCHMPQUEUE

La opción SEARCHMPQUEUE especifica el orden en el que el servidor da respuesta a las peticiones de la cola de montaje. Si se especifica la opción, el servidor primero intenta satisfacer las peticiones de los volúmenes que ya están montados. Estas peticiones pueden ser satisfechas antes que otras peticiones, aunque estas otras hayan estado esperando más tiempo el punto de montaje. Si no se especifica esta opción, el servidor satisface las peticiones en el orden en que éstas se reciben.

Sintaxis

```
>>-SEARCHMPQUEUE-----<<
```

Parámetros

Ninguno

Ejemplos

Especificar que el servidor intenta primero satisfacer una petición de un volumen que ya está montado:

```
searchmpqueue
```

 Sistemas operativos Windows

SECUREPIPES

Cuando se utiliza el protocolo Named Pipes, si se activa SECUREPIPES, el servidor se ve forzado a comprobar el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

El nombre del usuario y la contraseña definidos en el grupo Windows se utilizan para autenticar el nodo/usuario para acceder a los datos del servidor. El nodo/usuario también debe ser un nodo cliente de IBM Spectrum Protect registrado. Sin embargo, se pasa por alto la contraseña del nodo de cliente de IBM Spectrum Protect y se utiliza la contraseña de Windows asociada al usuario.

Sintaxis

```
>>-SECUREPipes--+Yes-+-----<<  
      '-No--'
```

Parámetros

Yes

Especifica que IBM Spectrum Protect comprueba el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

No

Especifica que IBM Spectrum Protect no comprueba el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

Ejemplos

Especificar que IBM Spectrum Protect compruebe el grupo Windows para autenticar los nodos cliente.

```
securepipes yes
```

SERVERDEDUPTXNLIMIT

La opción SERVERDEDUPTXNLIMIT especifica el tamaño máximo de los objetos que pueden tener optimización de almacenamiento en el servidor.

Cuando se usan proceso de identificación de duplicados (el mandato IDENTIFY DUPLICATES) para objetos de gran tamaño, puede producirse una actividad intensiva en la base de datos por las transacciones de ejecución larga necesarias para actualizar dicha base de datos. Unos niveles altos de actividad de la base de datos pueden producir los siguientes síntomas:

- Rendimiento reducido para las operaciones de copia de seguridad y de archivado del cliente
- Contienda de recursos debido a operaciones simultáneas del servidor
- Actividad excesiva del registro de recuperación

La medida en que se producen estos síntomas depende del número y del tamaño de los objetos que se procesan, de la intensidad y el tipo de las operaciones simultáneas que tienen lugar en el servidor de IBM Spectrum Protect y de la configuración de servidor de IBM Spectrum Protect.

Con la opción de servidor SERVERDEDUPTXNLIMIT es posible especificar un tamaño máximo, en gigabytes, para los objetos para los que se puede optimizar el almacenamiento. Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por SERVERDEDUPTXNLIMIT, los objetos no tienen optimización del almacenamiento por el servidor. Es posible especificar un valor de 32 a 102400 GB. El valor predeterminado es 5120 GB.

Aumentar el valor de esta opción hace que el servidor de IBM Spectrum Protect busque objetos aplazados anteriormente cuyo tamaño se encuentre por debajo del nuevo límite de transacción.

Recuerde: La búsqueda de objetos aplazados anteriormente puede llevar un tiempo. Tenga cuidado si aumenta el valor de SERVERDEDUPTXNLIMIT. Si se reduce el valor de esta opción, no se provoca que IBM Spectrum Protect busque objetos aplazados.

El valor adecuado para esta opción depende de la configuración de servidor de IBM Spectrum Protect y de la actividad simultánea del servidor. Es posible especificar un valor alto para esta opción si se minimiza la contienda de recursos. Para minimizar la contienda de recursos, realice operaciones como copia de seguridad, archivado, identificación de duplicados y reclamación en distintos momentos.

Para actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor, utilice el mandato SETOPT.

Sintaxis

```
.-5120-----.  
>>-SERVERDEDUPTXNlimit--+-gigabytes+-----<<
```

Parámetros

gigabytes



Especifica el tamaño máximo, en gigabytes, de los objetos que de los que se puede optimizar el almacenamiento en servidor. Es posible especificar un valor de 32 a 102400. El valor predeterminado es 5120.


Ejemplos

Inhabilitar la optimización de almacenamiento de datos en el lado del servidor para todos los objetos de más de 120 GB:

```
serverdeduptxnlimit 120
```

SHMPORT

 Sistemas operativos AIX  Sistemas operativos Linux La opción SHMPORT especifica la dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Todas las comunicaciones de memoria compartida comienzan por una conexión TCP/IP.




 Sistemas operativos Windows La opción SHMPORT especifica el puerto en el que el servidor está a la escucha de conexiones de memoria compartida.

Sintaxis

```
>>-SHMPort--número_puerto-----<<
```

Parámetros

número_puerto

Especifica el número de puerto.  Sistemas operativos AIX  Sistemas operativos Linux Puede especificar un valor de 1024 a 32767. El valor predeterminado es 1510.  Sistemas operativos Windows Puede especificar un valor de 1 a 32767. El valor predeterminado es 1.

Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

```
shmport 1580
```

 Sistemas operativos Windows

```
shmport 1
```

SHREDDING

La opción SHREDDING especifica si la destrucción de datos confidenciales suprimidos se lleva a cabo automática o manualmente. La destrucción sólo se aplica a los datos de las agrupaciones de almacenamiento que se han configurado explícitamente para dar soporte a la destrucción.

Sintaxis

```
>>-SHREDDing--+-AUTOMatic+-----<<
```

Parámetros

AUTOMATIC

Especifica que la destrucción se produzca automáticamente cuando se supriman datos confidenciales. Utilice esta opción para destruir datos confidenciales lo antes posible después de suprimirlos. Si no se especifica la opción SHREDDING, éste es el comportamiento predeterminado. Si se produce un error de E/S durante la destrucción automática, se notifica un error y se detiene la destrucción del objeto actual. Si el error de E/S no puede corregirse, es posible sea necesario ejecutar la destrucción manualmente y utilizar la palabra clave IOERROR.

MANUAL

Especifica que la destrucción se produce manualmente, sólo cuando se invoca el mandato SHRED DATA. Utilice esta opción para controlar cuando tiene lugar la destrucción para asegurarse de que no interfiera con otras actividades del servidor.

Consejo: Si especifica la destrucción manual, ejecute el mandato SHRED DATA con regularidad, como mínimo con la frecuencia con la que realiza otras tareas de mantenimiento rutinarias del servidor (por ejemplo, la caducidad, la reclamación, etc.). Esta práctica puede evitar la degradación del rendimiento que podrían experimentar determinados procesos del servidor (en particular, la migración). Para obtener resultados óptimos, ejecute SHRED DATA después de cualquier operación que suprima archivos de una agrupación de destrucción (por ejemplo, la caducidad y la migración).

Ejemplos

Especificar que IBM Spectrum Protect destruya automáticamente los datos de una agrupación de almacenamiento que se ha configurado para aplicar la destrucción tras haberse suprimido los datos:

```
shredding automatic
```

SNMPHEARTBEATINTERVAL

La opción SNMPHEARTBEATINTERVAL especifica el intervalo en minutos entre consultas del servidor de IBM Spectrum Protect.

Sintaxis

```
.-5-----.  
>>-SNMPHEARTBEATINTERVAL--+-minutos+-----<<
```

Parámetros

minutos

Especifica el intervalo de consultas en minutos. Los valores válidos son de 0 a 1440 (un día). El valor predeterminado es de 5 minutos.

Ejemplos

```
snmpheartbeatinterval 20
```

SNMPMESSAGECATEGORY

La opción SNMPMESSAGECATEGORY especifica los tipos de detecciones que se utilizan cuando se envían los mensajes desde el servidor, a través del subagente SNMP (Simple Network Management Protocol), al gestor SNMP.

Sintaxis

```
>>-SNMPMESSAGECATEGORY--+-SEVERITY---+-----<<  
                          '-INDIVIDUAL-'
```

Parámetros

SEVERITY

Especifica que existen cuatro tipos de detecciones basados en el nivel de gravedad de los mensajes.

- 1 Grave
- 2 Error
- 3 Aviso
- 4 Información

Este es el valor predeterminado.

INDIVIDUAL

Especifica que se utiliza un tipo de detección (de condición de excepción) para cada mensaje. La parte numérica del identificador de mensaje indica el tipo de detección (de condición de excepción).

Ejemplos

```
snmpmessagecategory individual
```

SNMPSUBAGENT

La opción SNMPSUBAGENT especifica los parámetros necesarios para que el subagente de IBM Spectrum Protect se comunique con el daemon SNMP (Simple Network Management Protocol). Esta opción únicamente sirve para configurar el subagente SNMP para las comunicaciones con el agente SNMP; el servidor la ignora.

Sintaxis

```
>>-SNMPSUBAGENT--+-+-----+-----+-----+----->
                    '-HOSTname -nombre_host-'
>--+-+-----+-----+-----+-----+-----+-----<<
    '-COMMunityname -nombre_comunidad-' '-TIMEOUT -segundos-'
```

Parámetros

HOSTname nombre_host

Especifica el nombre o número TCP/IP del host que ejecuta el agente SNMP con el que se conecta el subagente SNMP de IBM Spectrum Protect. Este parámetro es opcional. El nombre predeterminado es *localhost*.

COMMunityname nombre_comunidad

Especifica el nombre de comunidad configurado del sistema que se ejecuta en el agente SNMP. Este parámetro es opcional. El nombre predeterminado es *public*.

TIMEOUT segundos

Especifica el tiempo, en segundos, en el que debe recibirse una petición. Este parámetro es opcional. El valor predeterminado es 600.

Ejemplos

```
snmpsubagent hostname jimbo communityname public timeout 2600
```

SNMPSUBAGENTHOST

La opción SNMPSUBAGENTHOST especifica la ubicación del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect. El valor predeterminado para esta opción es 127.0.0.1.

Sintaxis

```
>>-SNMPSUBAGENTHOST--nombre_host-----<<
```

Parámetros

nombre_host

Especifica el nombre o número del host TCP/IP en el que está ubicado el subagente SNMP de IBM Spectrum Protect. El subagente y el servidor deben estar en el mismo nodo.

Ejemplos

```
snmpsubagenthost 9.116.23.450
```

SNMPSUBAGENTPORT

La opción SNMPSUBAGENTPORT especifica el número de puerto del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect.

Sintaxis

```
>>-SNMPSUBAGENTPORT--número_puerto-----><
```

Parámetros

número_puerto

Especifica el número de puerto del subagente SNMP de IBM Spectrum Protect. Los valores válidos son 1000 - 32767. El valor predeterminado es de 1521.

Ejemplos

```
snmpsubagentport 1525
```

SSLFIPSMODE

La opción SSLFIPSMODE especifica si se aplica la modalidad Estándar federal de procesamiento de información (FIPS) para la capa de sockets seguros (SSL). El valor predeterminado es NO.

Puesto que SSLv3 no está soportado por la modalidad FIPS, cuando se utiliza SSL con clientes de la versión 6.1 o V5.5, debe desactivar la modalidad FIPS.

Sintaxis

```
.-SSLFIPSMODE-----No-----.  
>>+-----+-----><  
'-SSLFIPSMODE-----+No--+-'  
      '-Yes-'
```

Parámetros

No

Especifica que la modalidad FIPS SSL no está activa en el servidor. Este valor es necesario cuando se van a conectar al servidor versiones del cliente de archivado y copia de seguridad anteriores a IBM Spectrum Protect 6.3 con SSL.

Sí

Un valor YES indica que la modalidad FIPS SSL está activa en el servidor. Este valor restringe la negociación de sesiones SSL al uso de suites de cifrado aprobadas por FIPS. Se recomienda especificar YES cuando la comunicación SSL está habilitada y todos los clientes de archivado y copia de seguridad se encuentran en V6.3 o posterior.

Para desactivar la modalidad FIPS SSL en el servidor:

```
SSLFIPSMODE no
```

SSLINITTIMEOUT

La opción SSLINITTIMEOUT especifica el tiempo, en minutos, que el servidor espera a que finalice la inicialización de una sesión SSL (capa de sockets seguros) antes de que cancelar la sesión.

Cuando especifica esta opción, la sesión SSL se cancela si un cliente, un servidor o un agente de almacenamiento no está configurado para SSL e intenta iniciar una sesión SSL. De forma parecida, la sesión SSL se cancela si la sesión SSL de cliente y el servidor no están configurados con la misma versión de TLS (seguridad de la capa de transporte). En estos casos, la sesión SSL no se inicializará completamente. El servidor cancela la sesión cuando se alcanza el tiempo de espera especificado.

Sintaxis

```
.-2-----.  
>>-SSLINITTIMEout--minutos+-----<<
```

Parámetros

minutos

Especifica el número máximo de minutos que el servidor espera a que una sesión SSL finalice la inicialización. El valor predeterminado es 2 minutos. El valor mínimo es de 1 minuto.

Ejemplo

```
sslinittimeout 1
```

SSLTCPADMINPORT

La opción SSLTCPADMINPORT especifica la dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera peticiones solo de sesiones con SSL habilitado. Las sesiones son para el cliente de administración de línea de mandatos.

Nota: A partir de IBM Spectrum Protect Versión 8.1.2 y Tivoli Storage Manager Versión 7.1.8, ya no es necesario utilizar la opción SSLTCPADMINPORT ni SSLTCPADMINPORT para permitir sesiones compatibles con SSL del cliente. El número de puerto especificado en la opción TCPADMINPORT o TCPADMINPORT escucha tanto a la sesión TCP/IP como a la sesión de cliente compatible con SSL.

Los siguientes tipos de sesiones no utilizan el protocolo de capa de sockets seguros (SSL):

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se establezcan números de puerto diferentes para las opciones SSLTCPADMINPORT y SSLTCPADMINPORT.

Restricciones:

Las restricciones siguientes se aplican cuando especifica los puertos de servidor solo SSL (SSLTCPADMINPORT y SSLTCPADMINPORT):

- Cuando especifique el puerto de servidor solo SSL para LLADDRESS en el mandato DEFINE SERVER o el mandato UPDATE SERVER, debe especificar también el parámetro SSL=YES.
- Cuando especifique el puerto de servidor solo SSL para la opción TCPADMINPORT del cliente, debe especificar también YES para la opción del cliente SSL.

El controlador de comunicaciones TCP/IP debe estar activado con COMMMETHOD TCPIP o COMMMETHOD V6TCPIP.

Sintaxis

```
>>-SSLTCPADMINPort--número_puerto-----<<
```

Parámetros

número_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. No existe un valor predeterminado.

Ejemplos

```
ssltcpadminport 1543
```

SSLTCPADMINPORT

La opción SSLTCPPOINT especifica el número de puerto de capa de sockets seguros (SSL) solo para las sesiones compatibles con SSL. La unidad de comunicación TCP/IP del servidor espera peticiones en este puerto para sesiones con SSL activada del cliente.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2 y Tivoli Storage Manager Versión 7.1.8, ya no es necesario utilizar la opción SSLTCPPOINT ni SSLTCPADMINPORT para permitir sesiones compatibles con SSL del cliente. El número de puerto especificado en la opción TCPPOINT o TCPADMINPORT escucha tanto a la sesión TCP/IP como a la sesión de cliente compatible con SSL.

Los siguientes tipos de sesiones no utilizan SSL:

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se establezcan números de puerto diferentes para las opciones SSLTCPADMINPORT y SSLTCPPOINT.

Si especifica el mismo número de puerto para las opciones SSLTCPPOINT y TCPPOINT, solo se aceptarán conexiones SSL y se inhabilitarán las conexiones TCP/IP para el puerto.

Restricciones:

Las restricciones siguientes se aplican cuando especifica los puertos de servidor solo SSL (SSLTCPPOINT y SSLTCPADMINPORT):

- Cuando especifique el puerto de servidor solo SSL para LLADDRESS en el mandato DEFINE SERVER o el mandato UPDATE SERVER, debe especificar también el parámetro SSL=YES.
- Cuando especifique el puerto de servidor solo SSL para la opción TCPPOINT del cliente, debe especificar también YES para la opción del cliente SSL.

El controlador de comunicaciones TCP/IP debe estar activado con COMMMETHOD TCP/IP o COMMMETHOD V6TCP/IP.

Sintaxis

```
>>-SSLTCPPOINT--número_puerto-----<<
```

Parámetros

número_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. No existe un valor predeterminado.

Ejemplos

```
ssltcpport 1542
```

TCPADMINPORT

La opción TCPADMINPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las peticiones de sesiones compatibles con TCP/IP y SSL distintas de las sesiones de cliente. Esto incluye las sesiones de administración, las sesiones de servidor a servidor, las sesiones del agente de almacenamiento, las sesiones del cliente de biblioteca, las sesiones de servidor gestionado y las sesiones del servidor de eventos.

La utilización de números de puerto distintos para las opciones TCPPOINT y TCPADMINPORT le permite crear un conjunto de reglas de cortafuegos para las sesiones de cliente y otro conjunto para los otros tipos de sesiones anteriormente indicados. Utilizando el parámetro SESSIONINITIATION de los mandatos REGISTER NODE y UPDATE NODE, puede cerrar el puerto especificado por TCPPOINT en el cortafuegos y especificar los nodos cuyas sesiones planificadas se iniciarán desde el servidor. Si los dos números de puerto son diferentes, se usan diferentes hebras para las sesiones de cliente de servicio y los tipos de sesión. Si admite las dos opciones para usar el mismo número de puerto (de forma predeterminada o al configurarlos explícitamente al mismo número de puerto), se usa un solo hilo del servidor para dar servicio a todas las solicitudes de sesión.

Las sesiones de cliente que intenten utilizar el puerto que especifica TCPADMINPORT terminarán (si TCPPOINT y TCPADMINPORT especifican puertos distintos). Se permitirán sesiones de administración en cualquiera de ambos puertos (a menos que la opción ADMINONCLIENTPORT se establezca en NO), pero de forma predeterminada utilizarán el puerto especificado por TCPADMINPORT.

Las sesiones compatibles con SSL que utilicen la opción TCPADMINPORT, tienen las mismas limitaciones que la opción SSLTCPADMINPORT. Los siguientes tipos de sesiones no utilizan el protocolo de capa de sockets seguros (SSL):

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)

- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se especifiquen número de puerto diferentes para las opciones TCPADMINPORT y TCPPOINT.

Sintaxis

```
>>-TCPADMINPort--número_puerto-----<<
```

Parámetros

número_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. El valor predeterminado es el valor de TCPPOINT.

Ejemplos

```
tcpadminport 1502
```

 Sistemas operativos AIX  Sistemas operativos Linux

TCPBUFSIZE

La opción TCPBUFSIZE especifica el tamaño del búfer utilizado para peticiones de envío TCP/IP. Durante una restauración, los datos de cliente se traspasan del componente de sesión IBM Spectrum Protect a un controlador de comunicaciones TCP. La opción TCPBUFSIZE determina si el servidor envía los datos directamente desde el búfer de la sesión o copia los datos en el búfer TCP. Un tamaño de búfer de 32 KB dará lugar a que servidor copie forzosamente los datos en su búfer de comunicaciones y al vaciado del búfer cuando éste esté lleno.

Nota: Esta opción no está relacionada con la opción TCPWINDOWSIZE.


Sintaxis

```
>>-TCPBufsize--kilobytes-----<<
```

Parámetros

kilobytes

Especifica el tamaño, en kilobytes, del búfer utilizado para peticiones de envío TCP/IP.

 Sistemas operativos AIX El rango de valores es de 1 a 64. El valor predeterminado es 32.

 Sistemas operativos Linux El rango de valores es de 1 a 64. El valor predeterminado es 16.

Ejemplos

```
tcpbufsize 5
```

TCPNODELAY

La opción TCPNODELAY especifica si el servidor inhabilita el retraso al enviar pequeños paquetes sucesivos en la red.

Cambie el valor predeterminado YES sólo en las condiciones siguientes:

- El representante del servicio le pide que cambie la opción.
- Comprende perfectamente las repercusiones del algoritmo Nagle TCP en las transmisiones por red. Si establece esta opción en NO, se habilitará el algoritmo Nagle, con lo que se retrasará el envío de pequeños paquetes sucesivos.

Sintaxis

```
>>-TCPNodelay--+-Yes+-----><
'-No--'
```

Parámetros

Yes

Especifica que el servidor permite el envío inmediato de pequeños paquetes sucesivos en la red. Si se establece esta opción en YES, el rendimiento de las redes de alta velocidad puede verse mejorado. El valor predeterminado es YES.

No

Especifica que el servidor no permite el envío inmediato de pequeños paquetes sucesivos en la red.

Ejemplos

```
tcpnodelay no
```

TCPPORT

La opción TCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. El controlador de comunicación TCP/IP de servidor escucha este puerto tanto para las sesiones TCP/IP como para las sesiones compatibles con SSL desde el cliente.


La utilización de números de puerto distintos para las opciones TCPPORT y TCPADMINPORT le permite crear un conjunto de reglas de cortafuegos para las sesiones de cliente y otro conjunto para los otros tipos de sesiones (sesiones de administración, sesiones de servidor a servidor, sesiones del agente de almacenamiento, sesiones del cliente de biblioteca, sesiones de servidor gestionado y sesiones del servidor de eventos). Si dos números de puerto son diferentes, se usan diferentes hilos para dar servicio a las sesiones del cliente y los otros tipos de sesión. Si admite las dos opciones para usar el mismo número de puerto (de forma predeterminada o al configurarlos explícitamente al mismo número de puerto), se usa un solo hilo del servidor para dar servicio a todas las solicitudes de sesión.

Las sesiones de cliente compatibles con SSL que utilicen la opción TCPPORT, tienen las mismas limitaciones que la opción SSLTCPPOINT. Los siguientes tipos de sesiones no utilizan SSL:

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSLs)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se especifiquen número de puerto diferentes para las opciones TCPADMINPORT y TCPPOINT.

Si especifica el mismo número de puerto para las opciones SSLTCPPOINT y TCPPOINT, solo se aceptarán conexiones SSL y se inhabilitarán las conexiones TCP/IP para el puerto.

 Sistemas operativos Windows Puede cambiar esta opción con el mandato SETOPT. Cuando cambia un puerto, el servidor de IBM Spectrum Protect inicia la escucha en el nuevo puerto de forma inmediata. Todas las conexiones permanecen en uso hasta que se cierran.

Sintaxis

```
>>-TCPPOINT--número_puerto-----><
```

Parámetros

número_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. El valor predeterminado es 1500.



```
tcpport 1500
```

TCPWINDOWSIZE

La opción TCPWINDOWSIZE especifica, en kilobytes, la cantidad de datos de recepción que se pueden almacenar en el búfer a la vez en una conexión TCP/IP. El host emisor no puede enviar más datos hasta que reciba una confirmación y una actualización de ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP anunciada en la conexión. Una ventana más grande

permite que el emisor continúe enviando datos y puede mejorar el rendimiento de las comunicaciones, sobre todo en las redes rápidas con una latencia elevada.

Nota:

- Para mejorar el rendimiento de las copias de seguridad, aumente TCPWINDOWSIZE en el servidor. Para mejorar el rendimiento en las operaciones de restauración, aumente TCPWINDOWSIZE en el cliente.
- La ventana TCP actúa como búfer en la red.
- Una ventana más grande que el espacio del búfer en el adaptador de la red puede disminuir el rendimiento debido al reenvío de los paquetes que se habían perdido en el adaptador.
-  Sistemas operativos AIX  Sistemas operativos Linux La opción TCPWINDOWSIZE no está relacionada con la opción TCPBUFFSIZE ni con los búferes de envío y recepción asignados en la memoria del cliente o del servidor.

Sintaxis

```
>>-TCPWindowsize--kilobytes-----<<
```

Parámetros

kilobytes

Especifica el tamaño, en kilobytes, que desea utilizar para la ventana de posición TCP/IP de su nodo cliente. Puede especificar un valor de 0 a 2048. El valor predeterminado es 63. Si se especifica 0, el servidor utiliza el tamaño de ventana predeterminado que establece el sistema operativo. Los valores de 1 a 2048 indican que el tamaño de ventana se encuentra dentro del rango de 1 KB a 2 MB.

Ejemplos

```
tcpwindowsize 63
```

TECBEGINEVENTLOGGING

La opción TECBEGINEVENTLOGGING especifica si las anotaciones de eventos del receptor de TIVOLI deben empezar cuando se inicie el servidor. Si se especifica la opción TECHOST, TECBEGINEVENTLOGGING toma de forma predeterminada el valor YES.

Sintaxis

```
>>-TECBegineventlogging--+-Yes+-----<<  
                        '-No--'
```

Parámetros

Yes

Especifica que la anotación de eventos se inicia al arrancar el servidor y si se ha especificado una opción TECHOST.

No

Especifica que cuando arranque el servidor no se iniciarán las anotaciones de eventos. Para iniciar más tarde las anotaciones de eventos en el receptor TIVOLI (si se ha especificado la opción TECHOST), debe emitir el mandato BEGIN EVENTLOGGING.

Ejemplos

```
tecbegineventlogging yes
```

TECHOST

La opción TECHOST especifica el nombre de host o dirección IP del servidor de eventos de Tivoli.

Sintaxis

```
>>-TECHost--nombre_host-----<<
```

Parámetros

nombre_host

Especifica el nombre de host o la dirección IP del servidor de eventos de Tivoli.

Ejemplos

```
techost 9.114.22.345
```

TECPORT

La opción TECPORT especifica la dirección de puerto TCP/IP en la que el servidor de eventos Tivoli está a la escucha. Esta opción sólo es necesaria si el servidor de eventos Tivoli se encuentra en un sistema que no tiene un servicio PortMapper en funcionamiento.

Sintaxis

```
>>-TECPort--numero_puerto-----<<
```

Parámetros

número_puerto

Especifica la dirección de puerto del servidor de eventos de Tivoli. El valor debe estar comprendido entre 0 y 32767.

 Sistemas operativos AIX  Sistemas operativos Linux Esta opción no es necesaria.

Ejemplos

```
tecport 1555
```

TECUTF8EVENT

La opción TECUTF8EVENT permite al administrador de IBM Spectrum Protect enviar información al servidor de Tivoli Enterprise Console (TEC) en formato de datos UTF-8. El valor predeterminado es No. Puede visualizar si esta opción está activada o no mediante la emisión del mandato QUERY OPTION.

Sintaxis

```
>>-TECUTF8event--+-Yes-+-----<<  
                '-No--'
```

Parámetros

Yes

Especifica que el servidor de IBM Spectrum Protect codificará el evento TEC en formato UTF-8 antes de emitir el evento al servidor TEC.

No

Especifica que el servidor de IBM Spectrum Protect no codificará el evento TEC en formato UTF-8 y se enviará al servidor TEC en formato ASCII.

Ejemplos

```
tecutf8event yes
```

THROUGHPUTDATATHRESHOLD

La opción THROUGHPUTDATATHRESHOLD especifica un umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele después de que se haya alcanzado el umbral de tiempo.

Esta opción se utiliza junto con la opción del servidor THROUGHPUTTIMETHRESHOLD, que establece el valor del umbral de tiempo más el tiempo de espera de medios. El umbral de tiempo se inicia cuando el cliente empieza a enviar datos al servidor para

almacenarlos (no cuando los configura o realiza el mantenimiento de los datos de la sesión).

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-THROUGHPUTDatathreshold--kilobytes_por_segundo-----<<
```

Parámetros

kilobytes_per_second

Especifica la productividad que deben alcanzar las sesiones de cliente para evitar que se cancelen después de que hayan transcurrido THROUGHPUTTIMETHRESHOLD minutos. Este umbral no incluye el tiempo de espera de los montajes de medios. Un valor de 0 impide examinar las sesiones de cliente debido a una productividad insuficiente. La productividad se calcula sumando los recuentos de bytes enviados y recibidos y dividiendo el resultado por la duración de la sesión. La duración no incluye el tiempo de espera de los montajes de medios y se empieza a contar a partir del momento en que el cliente envía datos al servidor para su almacenamiento. El valor predeterminado es 0. El valor mínimo es 0; el valor máximo es 99999999.

Ejemplos

Especificar que el servidor debe esperar hasta 90 minutos más el tiempo de espera del medio a partir del momento en que una sesión ha empezado a enviar datos antes de que el almacenamiento la examine como candidata a ser cancelada debido a una baja productividad. Si una sesión no alcanza una velocidad de transferencia de 50 KB por segundo, se cancelará.

```
throughputtimethreshold 90  
Throughputdatathreshold 50
```

THROUGHPUTTIMETHRESHOLD

La opción THROUGHPUTTIMETHRESHOLD especifica el umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

Sintaxis

```
>>-THROUGHPUTTimethreshold--minutos-----<<
```

Parámetros

minutos

Especifica el umbral para examinar sesiones de cliente y cancelarlas si no se alcanza el umbral de productividad de los datos (vea la opción de servidor THROUGHPUTDATATHRESHOLD). Este umbral no incluye el tiempo de espera de los montajes de medios. El umbral de tiempo se inicia cuando un cliente empieza a enviar datos al servidor para almacenarlos (no cuando los configura o realiza el mantenimiento de los datos de la sesión). El valor 0 impide examinar las sesiones de cliente debido a una baja productividad. El valor predeterminado es 0. El valor mínimo es 0; el valor máximo es 99999999.

Ejemplos

Especificar que el servidor debe esperar hasta 90 minutos más el tiempo de espera del medio a partir del momento en que una sesión ha empezado a enviar datos antes de examinarla como candidata a ser cancelada. Si una sesión no alcanza una velocidad de transferencia de 50 mil bytes por segundo, se cancelará.

```
throughputtimethreshold 90  
Throughputdatathreshold 50
```

 Sistemas operativos Windows

TIMEFORMAT

La opción TIMEFORMAT especifica el formato mediante el cual el servidor visualiza la hora.

El valor de TIMEFORMAT se altera temporalmente mediante la definición de formato de hora del entorno nacional si el entorno nacional se inicializa correctamente durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

Sintaxis

```
>>-TIMEformat--número_formato-----<<
```

Parámetros

número_formato

Seleccione un número de 1 a 4 para identificar el formato de hora que utiliza el servidor. El valor predeterminado es 1.

- | | |
|---|---------------------|
| 1 | hh:mm:ss |
| 2 | hh,mm,ss |
| 3 | hh.mm.ss |
| 4 | hh:mm:ss a.m o p.m. |
| 5 | a.m o p.m. hh:mm:ss |

Ejemplos

```
timeformat 4
```

TXNGROUPMAX

La opción TXNGROUPMAX especifica el número de objetos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones. El valor mínimo es de 4 objetos y el valor máximo es de 65000 objetos. El valor predeterminado son 4096 objetos. Los objetos transferidos son directorios, archivos reales o ambos. El servidor cuenta cada archivo o directorio como un objeto.

El rendimiento de las operaciones de copia de seguridad del cliente, de archivado, de restauración y de recuperación puede mejorarse utilizando un valor más alto para esta opción:

1. Si incrementa el valor de la opción TXNGROUPMAX especificando una cantidad mayor, verifique los posibles efectos que ello puede tener en las anotaciones de recuperación. La especificación de un valor más alto para la opción TXNGROUPMAX puede incrementar la utilización de las anotaciones de recuperación, así como el tiempo necesario para la validación de una transacción. Si los efectos son lo suficientemente significativos, pueden dar lugar a problemas en el funcionamiento del servidor.
2. Si se aumenta el valor de la opción TXNGROUPMAX, es posible que aumente la productividad de las operaciones que almacenan los datos directamente en la cinta, especialmente cuando se almacenan muchos objetos. Sin embargo, un valor mayor de la opción TXNGROUPMAX también puede aumentar el número de objetos que deben volver a enviarse en caso de que la transacción se detenga debido a que un archivo de entrada ha cambiado durante la realización de la copia de seguridad o porque se necesitaba un nuevo volumen de almacenamiento. Cuanto mayor sea el valor de la opción TXNGROUPMAX, más datos se volverán a enviar.
3. El aumento del valor TXNGROUPMAX afectará a la sensibilidad de detención de la operación y es posible que el cliente tenga que esperar más tiempo para que se complete la transacción.

Puede modificar el valor de esta opción para nodos cliente individuales. Consulte el parámetro TXNGROUPMAX en la REGISTER NODE (Inscribir un nodo) y la UPDATE NODE (Actualizar atributos del nodo).

Esta opción está relacionada con la opción TXNBYTELIMIT del archivo de opciones del cliente. TXNBYTELIMIT controla el número de bytes, y no el de objetos, que se transfieren entre los puntos de validación de transacciones. Al finalizar la transferencia de un objeto, el cliente valida la transacción si el número de bytes transferidos durante la transacción alcanza o sobrepasa el valor de TXNBYTELIMIT, independientemente del número de objetos transferidos.

Sintaxis

```
>>-TXNGroupmax--número_de_objetos-----><
```

Parámetros

number_of_objects

Especifica un número comprendido entre el 4 y el 65000 para el número máximo de objetos por transacción. El valor predeterminado es 4096.

Ejemplos

```
txngroupmax 4096
```

UNIQUETDPTEEVENTS

La opción UNIQUETDPTEEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect, incluidos los mensajes del cliente, del servidor y del cliente de IBM Spectrum Protect. El valor predeterminado es No.

Sintaxis

```
>>-UNIQUETDPteevents---+Yes+-----><  
      '-No--'
```

Parámetros

Yes

Especifica que los mensajes exclusivos de IBM Spectrum Protect Data Protection se envían al servidor de eventos TEC. Establece dinámicamente UNIQUETEEvents en YES.

No

Especifica que los mensajes generales se envían al servidor de eventos TEC.

Ejemplos

```
uniquetdpcevents yes
```

UNIQUETECEVENTS

La opción UNIQUETECEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect. El valor predeterminado es No.

Sintaxis

```
>>-UNIQUETEEvents---+Yes+-----><  
      '-No--'
```

Parámetros

Yes

Especifica que los mensajes exclusivos se envían al servidor de eventos TEC.

No

Especifica que los mensajes generales se envían al servidor de eventos TEC.

Ejemplos

```
uniquetecevents yes
```

USEREXIT

La opción USEREXIT especifica la salida definida por el usuario a la que se otorgará control para poder gestionar un evento.

Sintaxis

```
>>-USEREXIT---+Yes---nombre_módulo-----nombre_DLL----->
      '-No--'
      (1)          (2)
>--función-----><
```

Notas:

1. *nombre_módulo* sólo está disponible en AIX, HP-UX, Linux, Solaris y z/OS.
2. *nombre_DLL* sólo está disponible en Windows.
3. *función* sólo está disponible en Windows.



Parámetros



Yes



Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.


No


Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el mandato BEGIN EVENTLOGGING.


 Sistemas operativos AIX  Sistemas operativos Linux *nombre_módulo*


 Sistemas operativos AIX  Sistemas operativos Linux Especifica el nombre de módulo de la salida de usuario.

 Sistemas operativos AIX  Sistemas operativos Linux Es el nombre de una biblioteca compartida que contiene el programa de salida. El nombre de módulo puede ser un nombre de ruta totalmente calificado, o simplemente un nombre de módulo. Si se trata sólo del nombre de módulo, se carga desde el directorio actual.

 Sistemas operativos Windows *nombre_DLL*

 Sistemas operativos Windows Especifica el nombre DLL que contiene la función de salida de usuario.

 Sistemas operativos Windows *función*

 Sistemas operativos Windows Especifica el nombre de la función de salida de usuario de la DLL.

Ejemplos

 Sistemas operativos Windows

```
userexit yes dllname.dll dllmodulename
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
userexit yes fevent.exit
```

VERBCHECK

La opción VERBCHECK especifica que el servidor realizará una comprobación de errores adicional en la estructura de mandatos que el cliente ha enviado. Esta opción sólo debe habilitarse cuando el cliente envía al servidor solicitudes con un formato incorrecto, lo que provoca que el servidor se cuelgue. Cuando esta opción está habilitada, obtendrá un error de protocolo en lugar de que el servidor se cuelgue.

Sintaxis

```
>>-VERBCHECK-----><
```

Parámetros

Ninguno

Ejemplos

Habilita la comprobación de errores adicional de los mandatos que envía el cliente:

```
verbcheck
```

VOLUMEHISTORY

La opción VOLUMEHISTORY especifica los nombres de los archivos que se actualizarán automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor. No existe un valor predeterminado para esta opción.

Puede incluir una o varias opciones VOLUMEHISTORY en el archivo de opciones del servidor. Cuando utiliza varias opciones VOLUMEHISTORY, automáticamente el servidor actualiza y almacena una copia de seguridad de la información histórica de volúmenes en cada archivo que especifique.

Sintaxis

```
>>-VOLUMEHistory--nombre_archivo-----<<
```

Parámetros

nombre_archivo





Especifica el nombre del archivo en el que desea que el servidor almacene una copia de seguridad de la información histórica de volúmenes que recoja.

Ejemplos




```
volumehistory volhist.out
```


Herramientas del servidor

Utilice las herramientas del servidor para realizar tareas especiales en el servidor mientras éste no está en ejecución.

-  **Sistemas operativos Windows**DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)
Utilice el programa de utilidad DSMMAXSG para aumentar la longitud de transferencia máxima de los adaptadores de bus de host (HBA). Como resultado de ello, el tamaño de bloque que utiliza el servidor de IBM Spectrum Protect para la grabación de datos y para la obtención de datos de determinados tipos de unidades de cinta aumenta.
- **DSMSERV (Iniciar el servidor)**
Utilice este programa de utilidad para iniciar el servidor de IBM Spectrum Protect.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**Script de inicio del servidor: rc.dsmserv
Puede utilizar el script rc.dsmserv al arrancar el sistema para iniciar automáticamente una instancia de servidor con un ID de usuario específico.
-  **Sistemas operativos Linux**Script de inicio del servidor: dsmserv.rc
Puede utilizar el script dsmserv.rc para detener una instancia del servidor o para iniciar manual o automáticamente un servidor.
- **DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)**
Utilice este programa de utilidad para visualizar información sobre el espacio de almacenamiento definido para la base de datos. La salida de este programa de utilidad es la misma que la salida del mandato QUERY DBSPACE, pero puede utilizar este programa de utilidad cuando el servidor no se está ejecutando.
- **DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)**
Utilice este programa de utilidad para visualizar información sobre anotaciones de recuperación, incluidas las anotaciones activas, la duplicación para las anotaciones activas, el directorio de recuperación de errores para las anotaciones de archivado y la ubicación de desbordamiento para las anotaciones. Utilice este programa de utilidad cuando el servidor no esté en ejecución.
- **DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)**
Utilice este programa de utilidad para aumentar el espacio para la base de datos agregando directorios para que los utilice la base de datos. Este programa de utilidad realiza la misma función que el mandato EXTEND DBSPACE, pero puede utilizarlo cuando el servidor no esté ejecutándose.
- **DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)**
Utilice el programa de utilidad DSMSERV FORMAT para inicializar las anotaciones de recuperación y de base de datos del servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- **DSMSERV INSERTDB (Mover una base de datos de servidor a una base de datos vacía)**
Utilice el programa de utilidad DSMSERV INSERTDB para mover una base de datos del servidor a una nueva base de datos. La

base de datos puede extraerse del servidor original e insertarse en una nueva base de datos del nuevo servidor con una conexión de red entre los dos servidores. La base de datos también puede insertarse a partir de los medios que contienen la base de datos extraída.

- **DSMSERV LOADFORMAT (Formatear una base de datos)**
Utilice el programa de utilidad DSMSERV LOADFORMAT cuando actualice desde la Versión 5. El programa de utilidad formatea una base de datos vacía como preparación para insertar una base de datos extraída en la base de datos vacía.
- **DSMSERV REMOVEDB (Eliminar una base de datos)**
Utilice el programa de utilidad DSMSERV REMOVEDB para eliminar una base de datos de servidor de IBM Spectrum Protect.
- **DSMSERV RESTORE DB (Restaurar la base de datos)**
Utilice este programa de utilidad para restaurar una base de datos mediante una copia de seguridad de ésta.
-  **Sistemas operativos Windows DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)**
Utilice este programa de utilidad para crear entradas de registro para una instancia de servidor de IBM Spectrum Protect si las entradas se han suprimido accidentalmente.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)**
Utilice este mandato para capturar mensajes de consola de servidor de IBM Spectrum Protect a un archivo de anotaciones de usuario. Puede especificar que IBM Spectrum Protect grabe mensajes a más de un archivo de anotaciones de usuario.

 Sistemas operativos Windows

DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)

Utilice el programa de utilidad DSMMAXSG para aumentar la longitud de transferencia máxima de los adaptadores de bus de host (HBA). Como resultado de ello, el tamaño de bloque que utiliza el servidor de IBM Spectrum Protect para la grabación de datos y para la obtención de datos de determinados tipos de unidades de cinta aumenta.

Con este programa de utilidad, el tamaño máximo de bloque que se puede especificar es de 256 KB. En función del entorno del sistema, el aumento del tamaño de bloque puede mejorar la velocidad a que IBM Spectrum Protect procesa datos en operaciones de copia de seguridad y restauración, y de archivado y recuperación. Sin embargo, el programa de utilidad no afecta a la generación de conjuntos de copias de seguridad.

Tan solo pueden utilizarse unidades de cintas que estén conectadas a los HBA SCSI o de canal de fibra y que tienen los siguientes tipos de dispositivo:

- 3590
- 3592
- DLT
- ECARTRIDGE
- LTO

El programa de utilidad se ejecuta automáticamente como parte de la instalación del servidor de IBM Spectrum Protect y del agente de almacenamiento. Sin embargo, si instala un nuevo HBA en el sistema después de instalar un servidor o un agente de almacenamiento, o si instala una nueva versión de un controlador de dispositivo HBA existente que restablezca el valor del tamaño máximo de transferencia, deberá ejecutar manualmente el programa de utilidad para aprovechar el tamaño de bloque mayor.

Cuando se ejecuta este programa de utilidad, se modifica una clave del registro para cada controlador HBA del sistema. El nombre de la clave es MaximumSGList.

Restricción: Si se realiza una operación de copia de seguridad o de archivado de datos en cinta utilizando el tamaño de bloque de 256 KB y el HBA no da soporte a ese tamaño de bloque, no podrá agregar datos a la cinta ni leer datos de ella. Por ejemplo, si utiliza un sistema Windows de 256 KB para realizar la copia de seguridad de los datos del cliente en el servidor de IBM Spectrum Protect, no podrá restaurar los datos con un sistema Windows que dé soporte a una longitud de transferencia distinta. Para agregar datos o leer datos desde una cinta grabada con una longitud de transferencia de 256 KB, debe instalar un HBA que dé soporte a transferencias de 256 KB.

Sintaxis

```
>>-dsmmaxsg-----<<
```

Ejemplo: incrementar el tamaño de bloque para la grabación de datos



Ejecutar el programa de utilidad DSMMAXSG para aumentar el tamaño de bloque que utiliza IBM Spectrum Protect.

```
dsmmaxsg
```





-o archivo_opciones

Especifica un archivo de opciones para utilizarlo.

 Sistemas operativos AIX  Sistemas operativos Linux-quiet

 Sistemas operativos AIX  Sistemas operativos Linux Especifica que se suprimen los mensajes para la consola.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows MAINTenance

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica que el servidor se ha iniciado en modalidad de mantenimiento y que las planificaciones de mandatos administrativos, las planificaciones de cliente, las sesiones de cliente, la reclamación de espacio de almacenamiento, la caducidad del inventario y la migración de la agrupación de almacenamiento están inhabilitadas.

Consejo: La modalidad de mantenimiento es el método preferido para ejecutar el servidor durante las tareas de mantenimiento o reconfiguración. Cuando se ejecuta el servidor en modalidad de mantenimiento, las operaciones que pueden interrumpir las tareas de mantenimiento o reconfiguración se inhabilitan automáticamente.


RUNFILE nombre_archivo

Especifica el nombre de un archivo que debe ejecutarse en el servidor. El archivo contiene una lista de mandatos de servidor.


Atención: Cuando se utiliza el parámetro RUNFILE, el servidor se detiene cuando se completa el proceso. Debe reiniciar el servidor utilizando el programa de utilidad DSMSEV.

Ejemplo: iniciar el servidor

Inicie el servidor para un funcionamiento normal. Emita el siguiente mandato en una sola línea:

 Sistemas operativos AIX

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPsize=64K  
usr/bin/dsmsevr
```

 Sistemas operativos AIX asegúrese de incluir un espacio después de SHMPsize=64K. Al iniciar el servidor con este mandato, puede habilitar 64 KB de páginas de memoria para el servidor. Este valor permite optimizar el rendimiento del servidor.

 Sistemas operativos Linux

```
/opt/tivoli/tsm/server/bin/dsmsevr
```

 Sistemas operativos Windows

```
C:\Archivos de programa\Tivoli\TSM\bin\dsmsevr -k server2
```

 Sistemas operativos Windows

Ejemplo: iniciar otro servidor

Inicie un servidor adicional utilizando la clave de registro denominada SERVER2.


```
dsmsevr -k server2
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Ejemplo: cargar el script de ejemplo

Cargar el archivo de script de ejemplo que se proporciona con el servidor.

```
dsmsevr  
runfile scripts.smp
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows


Ejemplo: iniciar el servidor en modalidad de mantenimiento

Antes de iniciar las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento.

```
dsmsevr maintenance
```

Tareas relacionadas:

Inicio del servidor en modalidad de mantenimiento

 Sistemas operativos AIX

Script de inicio del servidor: rc.dsmsevr

Puede utilizar el script rc.dsmsserv al arrancar el sistema para iniciar automáticamente una instancia de servidor con un ID de usuario específico.

Sintaxis



```
>>-rc.dsmsserv--+- -u--nombre_usuario+----->
      '- -U--nombre_usuario-'

>--+-----><
  '- -i--dir_instancia-'
```

Parámetros

- u nombre_usuario
Especifica el ID de usuario de la instancia para la cual se ha configurado el entorno. El servidor se ejecutará con este ID de usuario.
- U nombre_usuario
Especifica el ID de usuario de la instancia para la cual se ha configurado el entorno. El servidor se ejecutará con el ID de usuario del invocador del mandato.
- i dir_instancia
Especifica un directorio de instancia, que se convierte en el directorio de trabajo del servidor.

Tareas relacionadas:

-  AIX: Inicio automático de servidores
-  Sistemas operativos Linux

Script de inicio del servidor: dsmsserv.rc

Puede utilizar el script dsmsserv.rc para detener una instancia del servidor o para iniciar manual o automáticamente un servidor.

Requisitos previos

Antes de emitir el mandato DSMSSERV.RC, complete los pasos siguientes:

1. Asegúrese de que la instancia de servidor se ejecuta bajo un ID de usuario no root con el mismo nombre que el propietario de la instancia.
2. Copie el script dsmsserv.rc en el directorio /etc/rc.d/init.d. El script dsmsserv.rc está en el directorio de instalación del servidor, por ejemplo, /opt/tivoli/tsm/server/bin.
3. Cambie el nombre del script de modo que coincida con el nombre del propietario de la instancia de servidor, por ejemplo, tsminst1.
4. Si el directorio de instancia de servidor no es directorio_inicio/tsminst1, localice la siguiente línea en la copia del script:

```
instance_dir="${instance_home}/tsminst1"
```

Cambie la línea para que apunte al directorio de instancia de servidor, por ejemplo:

```
instance_dir="/tsminst1"
```

5. En la copia del script, localice la línea siguiente:

```
# pidfile: /var/run/dsmsserv_instancename.pid
```

Cambie el valor del nombre de instancia por el nombre del propietario de la instancia del servidor. Por ejemplo, si el propietario de la instancia del servidor es tsminst1, actualice la línea como se muestra:

```
# pidfile: /var/run/dsmsserv_tsminst1.pid
```

6. Utilice herramientas como el programa de utilidad CHKCONFIG para configurar el nivel de ejecución en el que se inicia automáticamente el servidor. Especifique un valor que corresponda con una modalidad multiusuario, con el uso de redes habilitado. Generalmente, el nivel de ejecución que se utilizará es 2, 3 o 5, en función del sistema operativo y de su configuración. Para obtener más detalles sobre los niveles de ejecución, consulte la documentación de su sistema operativo.

Sintaxis

```
>>-dsmsserv.rc--+-+-----><
```

```

+-start----+
+-stop-----+
+-estado---+
'-restart-'

```

Parámetros


start
 Inicia el servidor.

stop
 Detiene el servidor.

status
 Muestra el estado del servidor. Si el estado es *iniciado*, el ID de proceso del proceso de servidor también se conoce.

restart
 Detiene el servidor y lo inicia de nuevo.

Tareas relacionadas:

 Linux: Inicio automático de servidores en sistemas Linux

DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)

Utilice este programa de utilidad para visualizar información sobre el espacio de almacenamiento definido para la base de datos. La salida de este programa de utilidad es la misma que la salida del mandato QUERY DBSPACE, pero puede utilizar este programa de utilidad cuando el servidor no se está ejecutando.

Sintaxis

```

>>-DSMSERV -+-----+----->
                | (1) |
                '----- -u--nombre_usuario-'

                (2) .- -k--Server1----- .
>-+-----+-----+-----+----->
    | (1) | | ' - -k -nombre_clave-'
    '----- -i--dir_instancia-'

>-+-----+-----+-----+-----+----->
    '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'











>-DISPlay DBSPace-----<<

```

Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux -u nombre_usuario
 Sistemas operativos AIX  Sistemas operativos Linux Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor.
-  Sistemas operativos AIX  Sistemas operativos Linux -i dir_instancia
 Sistemas operativos AIX  Sistemas operativos Linux Especifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows -k nombre_clave
 Sistemas operativos Windows Especifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo cuando exista más de un servidor en el mismo sistema. El valor predeterminado es SERVER1.
- o archivo_opciones**
 Especifica un archivo de opciones para utilizarlo.
- noexpire**
 Especifica que el proceso de caducidad se suprime durante el inicio.

-quiet

Especifica que se suprimen los mensajes para la consola.


Ejemplo: visualizar información acerca del espacio de base de datos

Visualizar información acerca del espacio de almacenamiento de la base de datos. Consulte la publicación Descripciones de los campos para obtener detalles sobre la información que aparece en la salida. Emita el mandato.

```
dsmserve display dbspace
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ubicación	Espacio total (MB)	Espacio utilizado (MB)	Espacio libre (MB)
/tsmdb001	46.080,00	20.993,12	25.086,88
/tsmdb002	46.080,00	20.992,15	25.087,85

 Sistemas operativos Windows

Ubicación	Espacio total (MB)	Espacio utilizado (MB)	Espacio libre (MB)
d:\tsm\db001	46.080,00	20.993,12	25.086,88
d:\tsm\db002	46.080,00	20.993,15	25.087,85

Descripciones de los campos

Ubicación

Directorio o ruta que se utiliza para almacenar la base de datos



Espacio total (MB)

Número total de megabytes de la ubicación

Espacio utilizado (MB)

Número de megabytes en uso en la ubicación

Espacio libre (MB)

 Sistemas operativos AIX  Sistemas operativos Linux Espacio que queda en el sistema de archivos en el que se encuentra la ruta

 Sistemas operativos Windows Espacio que queda en la unidad en la que se encuentra el directorio

DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)

Utilice este programa de utilidad para visualizar información sobre anotaciones de recuperación, incluidas las anotaciones activas, la duplicación para las anotaciones activas, el directorio de recuperación de errores para las anotaciones de archivado y la ubicación de desbordamiento para las anotaciones. Utilice este programa de utilidad cuando el servidor no esté en ejecución.











Sintaxis

```
>>-DSMSERV -+-----+----->
          | (1)
          |----- -u--nombre_usuario-|
          |
          | (2) .- -k--Server1-----
>+-----+-----+-----+----->
          | (1)
          |----- -i--dir_instancia-|
          |
          |----- -o--archivo_opciones-| - -noexpire-| - -quiet-|
>+-----+-----+-----+----->
>--DISPLAY LOG-----<
```

Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre_usuario
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir_instancia
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows-k nombre_clave
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. Utilice este parámetro sólo cuando exista más de un servidor en el mismo sistema. El valor predeterminado es SERVER1.
- o archivo_opciones
Especifica un archivo de opciones para utilizarlo.
- noexpire
Especifica que el proceso de caducidad se suprime durante el inicio.
- quiet
Especifica que se suprimen los mensajes para la consola.


Ejemplo: visualizar información de las anotaciones de recuperación

Visualizar información acerca de las anotaciones de recuperación. Consulte la publicación Descripciones de los campos para obtener detalles sobre la información que aparece en la salida.

```
dsmserv display log
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
    Espacio total(MB): 38.912
    Espacio utilizado(MB): 401.34
    Espacio libre(MB): 38.358,65
    Directorio anotaciones activas: /activelog
    Directorio anotaciones archivado: /archivelog
    Directorio anotaciones duplicadas: /mirrorlog
Directorio anotac. recuperación errores archivado: /archfailoverlog
```

 Sistemas operativos Windows

```
    Espacio total(MB): 38.912
    Espacio utilizado(MB): 401.34
    Espacio libre(MB): 38.358,65
    Directorio anotaciones activas: h:\tsm\activelog
    Directorio anotaciones archivado: k:\tsm\archivelog
    Directorio anotaciones duplicadas: i:\tsm\mirrorlog
Directorio de anotaciones de recuperación de errores de archivado: j:\tsm\archfailoverlog
```

Descripciones de los campos

Espacio total

Especifica el tamaño máximo de las anotaciones activas.

Espacio utilizado

Especifica la cantidad total del espacio de anotaciones activas que utiliza actualmente la base de datos, en megabytes.

Espacio libre

Especifica la cantidad de espacio de anotaciones activas en la base de datos que no se utiliza para transacciones sin validar, en megabytes.

Directorio de anotaciones activas

Especifica la ubicación donde se guardan los archivos de anotaciones activas. Cuando cambie el directorio de anotaciones activas, el servidor moverá todas las anotaciones archivadas al directorio de anotaciones de archivado y todas las anotaciones activas a un nuevo directorio de anotaciones activas.

Directorio anotaciones duplicadas

Especifica la ubicación en la que se mantiene la duplicación de las anotaciones activas.

Directorio de anotaciones de recuperación de errores de archivado

Especifica la ubicación en la que el servidor guarda las anotaciones de archivado si las anotaciones no se pueden archivar en el destino de las anotaciones de archivado.

DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)

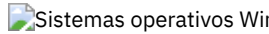
Especifica que los datos no se redistribuyan entre los directorios de base de datos y que no se pida espacio de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux

Ejemplo: aumentar el espacio para la base de datos

Añadir un directorio denominado stg1 en el directorio tsm_db para el espacio de almacenamiento de base de datos y, a continuación, redistribuir los datos y reclamar espacio emitiendo el mandato siguiente:

```
dsmserv extend dbSPACE /tsm_db/stg1
```

 Sistemas operativos Windows

Ejemplo: aumentar el espacio para la base de datos

Añadir la unidad D al espacio de almacenamiento para la base de datos y luego redistribuir los datos y reclamar almacenamiento emitiendo el mandato siguiente:

```
dsmserv extend dbSPACE D:
```

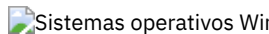
Referencia relacionada:

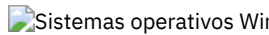
EXTEND DBSPACE (Incrementar el espacio para la base de datos)

DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)

Utilice el programa de utilidad DSMSERV FORMAT para inicializar las anotaciones de recuperación y de base de datos del servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Los directorios que se especifican en este programa de utilidad han de corresponder a almacenamiento rápido y fiable. No sitúe los directorios en sistemas de archivos que podrían quedarse sin espacio. Si determinados directorios (por ejemplo, el directorio de anotaciones activas), dejan de estar disponibles o se llenan, el servidor se detendrá.

 Sistemas operativos Windows Restricción: Si está utilizando una tabla de asignación de archivos (FAT o FAT32) o un formato New Technology File System (NTFS), no puede especificar el directorio raíz de dicho sistema como la ubicación de un directorio de base de datos o un directorio de registros. En su lugar, debe crear uno o varios subdirectorios dentro del directorio raíz. A continuación, cree los directorios de bases de datos y directorios de registros dentro de los subdirectorios.

 Sistemas operativos Windows Importante: El programa de instalación crea un conjunto de claves de registro. Una de estas claves señala al directorio en el que se crea el servidor predeterminado, denominado SERVER1. Para instalar un servidor adicional, cree un directorio y utilice el programa de utilidad DSMSERV FORMAT, con el parámetro -k, desde dicho directorio. Ese directorio se convierte en la ubicación del servidor. El registro realiza un seguimiento de los servidores instalados.

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

Sintaxis

```
>>-DSMSERV -+-----+----->
              | (1)           |
              '-u--nombre_usuario-'

              (2) .- -k--Server1-----.

>+-----+-----+-----+----->
  | (1)           |           | '- -k--nombre_clave-'
  '-i--dir_instancia-'

>+-----+-----+-----+----->
  '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'

              .-,-----
              v           |

>--FORMAT--+-DBDir---+----directorio+----->
              '-DBFile---+----archivo-----'

              .-ACTIVELOGSize---+----16384-----+
>+-----+-----+-----+----->
  '-ACTIVELOGSize---+----megabytes-'
```



```





>--ACTIVELOGDirectory---directory----->
>--ARCHLogdirectory---directory----->
>--+-----+----->
  '-ARCHFailoverlogdirectory---directory-'
>--+-----+-----<
  '-MIRRORlogdirectory---directory-'





```



Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

 Sistemas operativos AIX  Sistemas operativos Linux-u nombre_usuario
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor. Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Linux-i dir_instancia
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.

 Sistemas operativos Windows-k nombre_clave
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo para instalar servidores adicionales en el mismo sistema. Después de instalar un servidor mediante este parámetro, siempre debe iniciarlo con el valor de este parámetro. Este parámetro es opcional. El valor predeterminado es SERVER1.

Restricción: Las instancias adicionales del servidor IBM Spectrum Protect que se ejecuten en el mismo sistema competirán por los recursos y tendrán un impacto en el rendimiento general de cada servidor IBM Spectrum Protect.

-o archivo_opciones

Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.

-noexpire

Especifica que el proceso de caducidad se suprime durante el inicio. Este parámetro es opcional.

-quiet

Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.

DBDir

Especifica los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. Los nombres de directorio deben separarse mediante comas pero sin espacios. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

DBFile

Especifica el nombre de un archivo que contiene los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. El nombre de directorio de cada volumen debe estar en una línea aparte. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

ACTIVELOGSize

Especifica el tamaño del archivo de anotaciones activas en megabytes. Este parámetro es opcional. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16384 MB.

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Obligatorio)


```

>--INSERTDB---+| A: Inserción empleando medios |-----+----->
      '-| B: Inserción por medio de una red |- '

      .-PREview-----No-----
>+-----+-----><
      '-PREview-----+Yes-+-'
              '-No--'

A: Inserción empleando medios

|+-----+----->
      '-DEVclass---nombre_clase_dispositivo-'

      .-CONFiginfo---MANifest-----
>+-----+-----+-----|
      '-CONFiginfo---+MANifest-+-'
              '-DEVconfig-'

B: Inserción por medio de una red











      .-SESSWait---60-----
|+-----+-----|
      '-SESSWait---minutos-'



```



Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.


Parámetros

-  **Sistemas operativos AIX**  **Sistemas operativos Linux-u nombre_usuario**
 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor. Este parámetro es opcional.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux-i dir_instancia**
 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.
-  **Sistemas operativos Windows-k nombre_clave**
 **Sistemas operativos Windows** Especifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. Este parámetro es opcional. El valor predeterminado es SERVER1.
- o archivo_opciones**
 Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.
- noexpire**
 Especifica que el proceso de caducidad se suprime durante el inicio. Este parámetro es opcional.
- quiet**
 Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.
- DEVclass**
 Especifica una clase de dispositivo de acceso secuencial. Puede especificar cualquier clase de dispositivo excepto la clase de dispositivo DISK. La definición de la clase de dispositivo debe existir en el archivo de manifiesto o el archivo de configuración de dispositivo.
 Este parámetro es opcional y se utiliza sólo cuando la base de datos que desea insertar en la base de datos V8 vacía se ha extraído en medios. Si la base de datos se encuentra en un medio y no especifica una clase de dispositivo, se utiliza la clase de dispositivo identificada en el archivo de manifiesto.
 Restricción: No puede utilizar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA.
- MANifest**
 Especifica la ubicación del archivo de manifiesto. Utilice un nombre de archivo cualificado al completo o indique un directorio local. Por ejemplo: ./manifest.txt
 Este parámetro es necesario cuando la base de datos que desea insertar en la base de datos V8 vacía se ha extraído en medios.
- CONFiginfo**
 Especifica el origen de la información de configuración de dispositivo que ha utilizado la operación DSMSEV INSERTDB. El valor predeterminado para este parámetro es MANIFEST. Los valores posibles son los siguientes:
- MANifest**
 Especifica que la información de configuración de dispositivo se lee desde el archivo manifiesto. Si el archivo de manifiesto no tiene información de configuración de dispositivo, en su lugar se utiliza el archivo de configuración de

 Sistemas operativos AIX  Sistemas operativos Linux-i_dir_instancia

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.

 Sistemas operativos Windows-k nombre_clave

 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo para instalar servidores adicionales en el mismo sistema. Después de instalar un servidor mediante este parámetro, siempre debe iniciarlo con el valor de este parámetro. El valor predeterminado es SERVER1.

-o archivo_opciones

Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.

-noexpire

Especifica que el proceso de caducidad se suprime cuando se inicia el servidor. Este parámetro es opcional.

-quiet

Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.

DBDir

Especifica los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. Los nombres de directorio deben separarse mediante comas pero sin espacios. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

DBFile

Especifica el nombre de un archivo que contiene los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. El nombre de directorio de cada volumen debe estar en una línea aparte. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

ACTIVELOGSize

Especifica el tamaño del archivo de anotaciones activas en megabytes. Este parámetro es opcional. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16384 MB.

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Obligatorio)

Especifica el directorio en el que el servidor graba y almacena los archivos de registro activo. Sólo existe una ubicación de anotaciones activas. El nombre debe ser un nombre de directorio cualificado al completo. El directorio debe existir, debe estar vacío, y debe ser accesible mediante el ID de usuario del gestor de base de datos. El número máximo de caracteres es 175.

ARCHLogdirectory (Obligatorio)

Especifica el directorio para los archivos de anotaciones de archivado. El nombre debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

ARCHFailoverlogdirectory

Especifica el directorio que se utilizará como ubicación de almacenamiento alternativa si el directorio ARCHLOGDIRECTORY se llena. Este parámetro es opcional. El número máximo de caracteres es 175.

MIRRORlogdirectory

Especifica el directorio en el que el servidor duplicará las anotaciones activas (los archivos en el directorio ACTIVELOGDIRECTORY). Este parámetro es opcional. El directorio debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

Ejemplo: formatear una base de datos

 Sistemas operativos AIX  Sistemas operativos Linux

```
dmserv loadformat dbdir=/tsmdb001 activelogsiz=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

 Sistemas operativos Windows

```

dsmserve -k server2 loadformat dbdir=d:\tsm\db001 activelogsiz=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog

```

DSMSERV REMOVEDB (Eliminar una base de datos)

Utilice el programa de utilidad DSMSERV REMOVEDB para eliminar una base de datos de servidor de IBM Spectrum Protect.

Cuando ejecuta este programa de utilidad, se suprime la base de datos del servidor, los archivos de registro activo y los archivos de duplicación de registro activo. Sin embargo, los archivos de registro de archivado y archivos de registro de migración tras error del registro de archivado se suprimen sólo después de iniciar una restauración de base de datos en un punto en el tiempo.

El servidor de IBM Spectrum Protect debe detenerse antes de emitir este mandato.

Sintaxis

```

>>-DSMSERV -+-----+----->
            | (1) |
            '----- -u--nombre_usuario-'

(2) .- -k--Server1-----.
>-+-----+-----+----->
    | (1) | | '- -k--nombre_clave-'
    '----- -i--dir_instancia-'

>-+-----+-----+-----+----->
    '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'











. - -force==--No-----.
>--REMOVEDB--nombre_basedatos--><
    '- -force==--+-No--+-'
    '-Yes-'

```

Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre_usuario
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir_instancia
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows-k nombre_clave
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.
- o archivo_opciones
Especifica un archivo de opciones para utilizarlo.
- noexpire
Especifica que el proceso de caducidad se suprime durante el inicio.
- quiet
Especifica que se suprimen los mensajes para la consola.
- nombre_basedatos
El nombre de base de datos que se especificó durante la instalación. Si la base de datos se formateó manualmente, este es el parámetro de nombre de base de datos del programa de utilidad DSMSERV FORMAT o DSMSERV LOADFORMAT. Este nombre de base de datos también puede encontrarse en el archivo dsmserve.opt. Este parámetro es necesario.
- force
Especifica si se elimina la base de datos cuando hay conexiones abiertas. El valor predeterminado es No. Este parámetro es opcional. Los valores son los siguientes:
 - Yes
 - Especifica que la base de datos se elimine independientemente de las conexiones abiertas.
 - No

Especifica que la base de datos se elimine sólo cuando estén cerradas todas las conexiones.

Ejemplo: eliminar una base de datos

Eliminar la base de datos de servidor de IBM Spectrum Protect TSMDB1 y todas sus referencias.

```
dsmserv removedb TSMDB1
```

Ejemplo: eliminar una base de datos con el parámetro force

Elimine la base de datos de servidor de IBM Spectrum Protect TSMDB1 y todas sus referencias, aunque haya conexiones abiertas:

```
dsmserv removedb TSMDB1 force=yes
```

DSMSERV RESTORE DB (Restaurar la base de datos)

Utilice este programa de utilidad para restaurar una base de datos mediante una copia de seguridad de ésta.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

La operación de restauración utiliza copias de seguridad de base de datos creadas con el mandato BACKUP DB.

Importante: Tras una operación de restauración a un punto en el tiempo específico, emita el mandato AUDIT VOLUME para auditar todos los volúmenes de DISK y resolver cualquier incoherencia entre la información de la base de datos y los volúmenes de agrupación de almacenamiento. Antes de restaurar la base de datos, examine el archivo histórico de volúmenes para averiguar los volúmenes de agrupaciones de almacenamiento de acceso secuencial que se suprimieron o reutilizaron desde el momento en el que se restauró la base de datos.

- DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)
Utilice el programa de utilidad DSMSERV RESTORE DB para restaurar una base de datos a su estado más actualizado cuando se dan determinadas condiciones.
- DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)
Utilice este mandato para restaurar una base de datos a momento anterior. Un archivo de historial de volumen y un archivo de configuración de dispositivo deben estar disponibles.

DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)

Utilice el programa de utilidad DSMSERV RESTORE DB para restaurar una base de datos a su estado más actualizado cuando se dan determinadas condiciones.

Deben satisfacerse las condiciones siguientes:

- Existe un archivo histórico de volúmenes intacto disponible.
- Las anotaciones de recuperación están disponibles.
- Existe un archivo de configuración de dispositivo con la información de dispositivo aplicable disponible.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

IBM Spectrum Protect solicita que los montajes de volúmenes carguen la serie de copias de seguridad más reciente y, a continuación, utiliza las anotaciones de recuperación para actualizar la base de datos a su estado más actual.

Las copias de seguridad de instantáneas de la base de datos no pueden utilizarse para restaurar una base de datos a su estado más actual.

Sintaxis

```
>>-DSMSERV -+-----+----->
            | (1)
            '----- -u--nombre_usuario-'
```

```

(2) .- -k--Server1-----
>-----+-----+-----+-----+-----+-----+-----+-----+----->
| (1) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----- -i--dir_instancia-' | | | | | | | | | | | | | | | | | | | | | | |
|-----+-----+-----+-----+-----+-----+-----+-----+----->
'- -o--archivo_opciones-' | (1) | | | | | | | | | | | | | | | | | | | | | | |
|-----+-----+-----+-----+-----+-----+-----+-----+----->
'-RECOVerrydir-----directorio-'
|-----+-----+-----+-----+-----+-----+-----+-----+----->
'-ACTIVELOGDir-----directorio-'
|-----+-----+-----+-----+-----+-----+-----+-----+----->
'-ON-----archivo_directorio_destino-'
.-PREview-----No----- .-RESTOREKeys-----No-----
>-----+-----+-----+-----+-----+-----+-----+-----+----->
'-PREview-----+Yes--+-' | | | | | | | | | | | | | | | | | | | | | | |
|-----+-----+-----+-----+-----+-----+-----+-----+----->
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----+-----+-----+-----+-----+-----+-----+-----+----->
'-PASSword-----nombre_contraseña-'

```

Notas:

- 1. Este parámetro solo se aplica a los servidores AIX y Linux.
- 2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

Sistemas operativos AIX **Sistemas operativos Linux-u nombre_usuario**
Sistemas operativos AIX **Sistemas operativos Linux** Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor.

Sistemas operativos AIX **Sistemas operativos Linux-i dir_instancia**
Sistemas operativos AIX **Sistemas operativos Linux** Especifica un directorio de instancia para utilizarlo. Este directorio de instancia se convierte en el directorio de trabajo actual del servidor.

Sistemas operativos Windows-k nombre_clave
Sistemas operativos Windows Especifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.

-o archivo_opciones
 Especifica un archivo de opciones para utilizarlo.

Sistemas operativos AIX **Sistemas operativos Linux-quiet**
Sistemas operativos AIX **Sistemas operativos Linux** Especifica que se suprimen los mensajes para la consola.

RECOVerrydir
 Especifica un directorio donde almacenar la información de anotaciones de recuperación a partir de los soportes de copia de seguridad de la base de datos. Este directorio debe tener espacio suficiente para contener la información de recuperación de transacciones y debe ser un directorio vacío. Si no se especifica este parámetro, el valor predeterminado es el directorio especificado por uno de los parámetros siguientes en el programa de utilidad DSMSERV FORMAT o DSMSERV LOADFORMAT:

- ARCHFAILOVERLOGDIRECTORY, si se especifica
- ARCHLOGDIRECTORY, si no se ha especificado ARCHFAILOVERLOGDIRECTORY

ACTIVELOGDir
 Especifica un directorio donde almacenar los archivos de anotaciones que se utilizan para rastrear las operaciones de la base de datos activas. Este directorio sólo debe especificarse si se tiene la intención de cambiar a un directorio de registros activos diferente del que ya se ha configurado.

On
 Especifica un archivo que contiene un listado de los directorios en los que se restaurará la base de datos. Especifique cada directorio en una línea separada del archivo. Por ejemplo, el parámetro ON especifica el archivo restorelist.txt que contiene la lista siguiente: **Sistemas operativos AIX** **Sistemas operativos Linux**

```

/t.smdb001
/t.smdb002
/t.smdb003

```

Sistemas operativos Windows

e:\t\sm\db001
f:\t\sm\db002
g:\t\sm\db003

Si no se especifica este parámetro, se utilizarán los directorios originales que se registraron en la copia de seguridad de la base de datos.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

PReview

Especifica que los archivos de historial de volumen se examinarán y que los volúmenes de copia de seguridad de base de datos del archivo de historial de volumen se evaluarán.

1. ¿Qué conjunto de volúmenes de copia de seguridad de base de datos cumple mejor los criterios más actualizados que se han especificado para el proceso de restauración? La información de historial de volumen proporciona detalles sobre el ID de serie de copias de seguridad, el ID de operación (completo, incremental 1, incremental 2, etc.), la fecha de la copia de seguridad de la base de datos, y la clase de dispositivo. Esta información y los parámetros especificados en el mandato DSMSERV RESTORE DB determinan qué se utiliza para realizar la restauración. El archivo de historial de volumen se examina para buscar la copia de seguridad de base de datos más reciente y restaurar los datos utilizando esa copia de seguridad.
2. ¿Hay disponibles datos autodescriptivos para el conjunto seleccionado de volúmenes de copia de seguridad de base de datos? Coteje la información de historial de volumen para esta serie de copias de seguridad. La reconciliación notifica qué contienen los datos autodescriptivos comparados con los datos obtenidos de las entradas del historial de volumen. El cotejo implica montar uno o varios de los volúmenes indicados en el historial de volumen. A continuación, utilizando los datos autodescriptivos que se han incluido en los volúmenes de copia de seguridad de base de datos, esa información se reconcilia con los datos del historial de volumen de la copia de seguridad de base de datos. Si la información del archivo de historial de volumen es incoherente con los datos autodescriptivos, se emiten mensajes para identificar el problema. Por ejemplo, no todos los valores se han especificado y están disponibles, y no se encuentran datos autodescriptivos.


Si la información del historial de volumen es coherente con los datos autodescriptivos de la copia de seguridad de base de datos, se emite un mensaje indicando que la copia de seguridad de base de datos puede utilizarse para procesos de restauración.




Si la información del historial de volumen no es coherente con los datos autodescriptivos de la copia de seguridad de base de datos o si no se encuentran datos autodescriptivos para la copia de seguridad, se emiten mensajes de error indicando qué se ha comprobado y qué faltaba.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y si el historial de volumen y los datos autodescriptivos de la copia de seguridad de la base de datos son coherentes, la restauración continúa.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y la reconciliación y la validación fallan, no se realiza la restauración de la base de datos. Haga que haya más volúmenes disponibles y haga referencia a ellos desde el archivo de historial de volumen, o elimine la operación o la serie de copias de seguridad para que el servidor de IBM Spectrum Protect seleccione una operación o serie preferida diferente y continúe el proceso.

Si el parámetro PREVIEW está definido en YES, el proceso solo ejecuta la evaluación del archivo de historial de volumen y la reconciliación y validación con la copia de seguridad de base de datos seleccionada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows RESTOREKeys

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica si se debe restaurar la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento cuando se restaura la base de datos. Este parámetro es opcional y solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno en la nube. Si la clave maestra de servidor está protegida cuando se restaura la base de datos, el valor predeterminado es YES. Si la clave maestra de servidor no está protegida cuando se restaura la base de datos, el valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que la clave maestra de servidor no se restaura cuando se restaura la base de datos.




Yes

Especifica que la clave maestra de servidor se restaura cuando se restaura la base de datos. Debe especificar una contraseña con este parámetro.

Only

Especifica que sólo se restaura la clave maestra del servidor. La base de datos no se restaura.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PASSWORD

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. Este parámetro solo se aplica si está utilizando agrupaciones de

almacenamiento de contenedores cifradas en un entorno de nube. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos. Debe utilizar una contraseña si especifica el parámetro RESTOREKEYS=YES o RESTOREKEYS=ONLY.

Ejemplo: restaurar la base de datos a su estado más actualizado

Restaurar la base de datos a su estado más actual utilizando el directorio de registro activo que ya está configurado.

```
dsmserv restore db
```

Ejemplo: Restaurar la clave maestra del servidor sin restaurar la base de datos

Para restaurar la clave maestra del servidor sin restaurar la base de datos, emita el siguiente mandato:

```
dsmserv restore db restorekeys=only
```

DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)

Utilice este mandato para restaurar una base de datos a momento anterior. Un archivo de historial de volumen y un archivo de configuración de dispositivo deben estar disponibles.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

Las copias de seguridad de bases de datos completas e incrementales o las copias de seguridad de instantáneas de bases de datos pueden utilizarse para restaurar una base de datos a un punto en el tiempo específico.

Consejo: Cuando se restaura una base de datos del servidor de IBM Spectrum Protect V7 o posterior a un punto específico en el tiempo, el método preferido es emitir el mandato DSMSERV REMOVE DB antes de emitir el mandato DSMSERV RESTORE DB. De este modo se garantiza que el sistema está en un estado limpio. El sistema elimina y descataloga la base de datos en segundo plano. Al restaurar datos a un punto específico en el tiempo, todos los registros necesarios y la imagen de base de datos se recuperan de los medios de copia de seguridad.

Sintaxis

```
>>-DSMSERV -+-----+----->
              | (1) |
              '----- -u--nombre_usuario-'
              (2).- -k--Server1-----.
>-+-----+-----+----->
  | (1) | | | '- -k--nombre_clave-'
  '----- -i--dir_instancia-'
>-+-----+-----+-----RESTORE DB----->
  '- -o--archivo_opciones-' | (1) |
                          '----- -quiet-'
                          .-Totime----23:59:59-.
>--Todate----fecha--+-----+----->
                          '-Totime----hora-----'
                          .-Source----DBBackup-----.
>-+-----+-----+----->
  '-Source----+DBBackup---+-'
                  '-DBSnapshot-'
>-+-----+-----+----->
  '-RECOVerydir----directorio-'
>-+-----+-----+----->
  '-ACTIVELOGDir----directorio-'
>-+-----+-----+----->
  '-ON----archivo_directorio_destino-'
```

```

.-PReview-----No----- .-RESTOREKeys-----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-PReview-----+Yes-+-' '-RESTOREKeys-----+No-+-'
      '-No--'           +-YES--+
                        '-ONLY-'











>+-----+-----+-----+-----+-----+-----+-----+-----><
'-PASSword-----nombre_contraseña-'

```

Notas:





1. Este parámetro se aplica solo a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre_usuario
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al que cambiar antes de iniciar el servidor.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir_instancia
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows-k nombre_clave
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.

-o archivo_opciones

Especifica un archivo de opciones para utilizarlo.

-  Sistemas operativos AIX  Sistemas operativos Linux-quiet
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica que se suprimen los mensajes para la consola.

TODate (Obligatorio)

Especifica la fecha en la que debe restaurarse la base de datos. Son posibles los valores siguientes:

MM/DD/AAAA

Especifica que desea restaurar una base de datos utilizando la última serie de copias de seguridad creada antes de la fecha especificada.

TODAY

Especifica que desea restaurar una base de datos utilizando la serie de copias de seguridad más reciente creada antes de hoy.

TODAY-número_días o -número_días

Especifica que desea restaurar una base de datos utilizando la serie de copias de seguridad más reciente que fue creado en el número de días especificado antes de la fecha actual.

TOTime

Especifica el momento del día en el que debe restaurarse la base de datos. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Los valores posibles son:

HH:MM:SS

Especifica que desea restaurar la base de datos utilizando la última serie de copias de seguridad creada en el momento especificado o antes en la fecha que se especifica en el parámetro TODATE.

NOW

Especifica que desea restaurar la base de datos utilizando una serie de copias de seguridad creada en el momento especificado o antes en la fecha que se especifica en el parámetro TODATE.

Por ejemplo, si emite el programa de utilidad DSMSERV RESTORE DB a las 9:00 con TOTIME=NOW, la base de datos se restaura utilizando la última serie de copias de seguridad creada a las 9:00 o antes en la fecha especificada en el parámetro TODATE.

NOW-número_horas:número_minutos o -número_horas:número_minutos

Especifica que desea restaurar la base de datos utilizando una serie de copias de seguridad creada en el momento actual o antes menos un número especificado de horas y, opcionalmente, minutos en la fecha que se especifica en el parámetro TODATE.

Por ejemplo, si emite el programa de utilidad DSMSERV RESTORE DB a las 9:00 con TOTIME=NOW-3:30, la base de datos se restaura utilizando la última serie de copias de seguridad creada a las 5:30 o antes en la fecha especificada en el parámetro TODATE.

Source

Especifica si la base de datos se restaura mediante volúmenes de copia de seguridad incrementales o completas de la base de datos o mediante volúmenes de instantánea de base de datos. Este parámetro es opcional. El valor predeterminado es DBBackup. Son posibles los valores siguientes:

DBBackup

Especifica que la base de datos se restaure del siguiente modo:

1. Lee el archivo histórico de volúmenes para localizar los volúmenes de copia de seguridad incremental y completa de la base de datos necesarios.
2. Solicita montajes y carga datos de los volúmenes de copia de seguridad incremental y completa de la base de datos que necesarios para restaurar el volumen de base de datos al momento especificado.

DBSnapshot

Especifica que la base de datos se restaure del siguiente modo:

1. Lee el archivo histórico de volúmenes para localizar los volúmenes de instantánea de base de datos necesarios,
2. Solicita montajes y carga datos de los volúmenes de instantánea de base de datos que necesita para restaurar el volumen al momento especificado.

RECOVdir

Especifica un directorio donde almacenar la información de anotaciones de recuperación a partir de los soportes de copia de seguridad de la base de datos. Esta información de anotaciones se utiliza para establecer la coherencia de las transacciones de la base de datos del servidor como parte del proceso de recuperación. Este directorio debe tener espacio suficiente para contener la información de recuperación de transacciones y debe ser un directorio vacío. Si el parámetro no se especifica, el valor predeterminado es el directorio especificado por uno de los parámetros siguientes en el programa de utilidad DSMSEV FORMAT o DSMSEV LOADFORMAT:

- ARCHFAILOVERLOGDIRECTORY, si se especifica
- ARCHLOGDIRECTORY, si no se ha especificado ARCHFAILOVERLOGDIRECTORY


ACTIVELOGDir

Especifica un directorio donde almacenar los archivos de anotaciones que se utilizan para rastrear las operaciones de la base de datos activas. Especifique este directorio sólo si se tiene intención de conmutar a un directorio de anotaciones activas diferente del que ya se ha configurado.

On

Especifica un archivo que contiene un listado de los directorios en los que se restaurará la base de datos. Especifique cada directorio en una línea separada del archivo. Por ejemplo, el parámetro ON especifica el archivo restorelist.txt que contiene la lista siguiente:

```
/t smdb001  
/t smdb002  
/t smdb003
```

 Sistemas operativos Windows

```
e: \t sm\ db001  
f: \t sm\ db002  
g: \t sm\ db003
```

Si no se especifica este parámetro, se utilizarán los directorios originales que se registraron en la copia de seguridad de la base de datos.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

PReview

Especifica que los archivos de historial de volumen se examinarán y que los volúmenes de copia de seguridad de base de datos del archivo de historial de volumen se evaluarán.

1. ¿Qué conjunto de volúmenes de copia de seguridad de base de datos cumple mejor los criterios de instante específico que se han especificado para el proceso de restauración? La información de historial de volumen proporciona detalles sobre el ID de serie de copias de seguridad, el ID de operación (completo, incremental 1, incremental 2, etc.), la fecha de la copia de seguridad de la base de datos, y la clase de dispositivo. Esta información y los parámetros especificados en el mandato DSMSEV RESTORE DB determinan qué se utiliza para realizar la restauración. El archivo de historial de volumen se examina para buscar la copia de seguridad de base de datos que mejor cumpla los criterios de instante específico y realizar a continuación la restauración utilizando esa copia de seguridad.
2. ¿Hay disponibles datos autodescriptivos para el conjunto seleccionado de volúmenes de copia de seguridad de base de datos? Coteje la información de historial de volumen para esta serie de copias de seguridad. La reconciliación notifica qué

contienen los datos autodescriptivos comparados con los datos obtenidos de las entradas del historial de volumen. El cotejo implica montar uno o varios de los volúmenes indicados en el historial de volumen. A continuación, utilizando los datos autodescriptivos que se han incluido en los volúmenes de copia de seguridad de base de datos, esa información se reconcilia con los datos del historial de volumen de la copia de seguridad de base de datos. Si la información del archivo de historial de volumen es incoherente con los datos autodescriptivos, se emiten mensajes para identificar el problema. Por ejemplo, no todos los valores se han especificado y están disponibles, y no se encuentran datos autodescriptivos.

Si la información del historial de volumen es coherente con los datos autodescriptivos de la copia de seguridad de base de datos, se emite un mensaje indicando que la copia de seguridad de base de datos puede utilizarse para procesos de restauración.




Si la información del historial de volumen no es coherente con los datos autodescriptivos de la copia de seguridad de base de datos o si no se encuentran datos autodescriptivos para la copia de seguridad, se emiten mensajes de error indicando qué se ha comprobado y qué faltaba.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y si el historial de volumen y los datos autodescriptivos de la copia de seguridad de la base de datos son coherentes, la restauración continúa.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y la reconciliación y la validación fallan, no se realiza la restauración de la base de datos. Haga que haya más volúmenes disponibles y haga referencia a ellos desde el archivo de historial de volumen, o elimine la operación o la serie de copias de seguridad para que el servidor de IBM Spectrum Protect seleccione una operación o serie preferida diferente y continúe el proceso.

Si el parámetro PREVIEW está definido en YES, el proceso solo ejecuta la evaluación del archivo de historial de volumen y la reconciliación y validación con la copia de seguridad de base de datos seleccionada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
Especifica si se debe restaurar la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento cuando se restaura la base de datos. Este parámetro es opcional y solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno en la nube. Si la clave maestra de servidor está protegida cuando se restaura la base de datos, el valor predeterminado es YES. Si la clave maestra de servidor no está protegida cuando se restaura la base de datos, el valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No


Especifica que la clave maestra de servidor no se restaura cuando se restaura la base de datos.




Yes

Especifica que la clave maestra de servidor se restaura cuando se restaura la base de datos. Debe especificar una contraseña con este parámetro.

Only

Especifica que sólo se restaura la clave maestra del servidor. La base de datos no se restaura.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. Este parámetro solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno de nube. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos. Debe utilizar una contraseña si especifica el parámetro RESTOREKEYS=YES o RESTOREKEYS=ONLY.

Ejemplo: restaurar la base de datos a un instante específico

Restaura la base de datos al estado que tenía el 12 de mayo de 2011 a las 14:25 horas.

```
dsmserv restore db todate=05/12/2011 totime=14:45
```

Ejemplo: Restaurar la clave maestra del servidor sin restaurar la base de datos

Para restaurar la clave maestra del servidor sin restaurar la base de datos, emita el siguiente mandato:

```
dsmserv restore db restorekeys=only
```

 Sistemas operativos Windows

DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)

Utilice este programa de utilidad para crear entradas de registro para una instancia de servidor de IBM Spectrum Protect si las entradas se han suprimido accidentalmente.

Ejecute este programa de utilidad del directorio de instancia para la base de datos (donde archivos tales como dmserv.dsk se almacenan para el servidor). El programa de utilidad vuelve a crear las entradas de registro originales para el servidor.

Sintaxis

```
      .- -k--Server1-----.  
>>-DSMSERV--+-+-----+---UPDATE----->>  
      '- -k--nombre_clave-'
```

Parámetros

-k nombre_clave

Especifica el nombre de la clave de registro de Windows en la que ha de almacenarse información acerca del servidor. El valor predeterminado es Server1.

Ejemplo: volver a crear entradas de registro para una instancia de servidor

Ejecute el programa de utilidad para volver a crear entradas de registro para la instancia de servidor, Server2.

```
"c:\Archivos de programa\Tivoli\TSM\server\bin\dmserv" -k server2 update
```

 Sistemas operativos AIX  Sistemas operativos Linux

DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)

Utilice este mandato para capturar mensajes de consola de servidor de IBM Spectrum Protect a un archivo de anotaciones de usuario. Puede especificar que IBM Spectrum Protect grabe mensajes a más de un archivo de anotaciones de usuario.

Importante: No coloque las anotaciones de usuario en los sistemas de archivos /usr u /opt porque existen restricciones de espacio en el sistema de archivos que pueden impedir que el servidor se inicie.

Sintaxis

```
      .-,-----  
      v |  
>>-DSMULOG----nombre_archivo_anotaciones-+----->>
```

Parámetros

nombre_archivo_anotaciones (Necesario)

Especifica el nombre de uno o varios archivos de anotaciones de usuario en los que IBM Spectrum Protect guarda mensajes de consola del servidor. Cuando especifique varios nombres de archivo, se graba en cada archivo durante un día y, a continuación, el servidor se mueve al siguiente archivo para capturar mensajes de anotaciones. Cuando todos los archivos de la lista se hayan grabado, el servidor comenzará a escribir en el primer archivo de nuevo y todos los mensajes contenidos en él se sobrescribirán.

Ejemplo: capturar mensajes de la consola de servidor en un archivo de anotaciones de usuario diariamente

Especifique los archivos de anotaciones de usuario en los que desee registrar los mensajes de la consola.




En este ejemplo, si invoca este programa de utilidad el viernes, los mensajes de servidor se capturan en log1 el viernes, los mensajes se capturan en log2 el sábado y los mensajes se capturan en log3 el domingo. El lunes, los mensajes se capturan en log1 y los mensajes del viernes anterior se sobrescriben.


```
/opt/tivoli/tsm/server/bin/dmserv -u tsminst1 -i  
/tsmserv/tsminst1/tsminst1 2>&1 | dsmulog /tsmserv/tsminst1/tsminst1/log1  
/tsmserv/tsminst1/tsminst1/log2  
/tsmserv/tsminst1/tsminst1/log3 &
```

Programas de utilidad de dispositivos de servidor de IBM Spectrum Protect

Puede utilizar los programas de utilidad de dispositivo para las tareas relacionadas con la configuración de dispositivos de almacenamiento para el servidor.

Programas de utilidad de dispositivo

-  Sistemas operativos AIXtsmdlst (Visualizar información sobre dispositivos)
-  Sistemas operativos Linuxautoconf (dispositivos de configuración automática)
-  Sistemas operativos Windowstsmldst (Visualizar información sobre dispositivos)

 Sistemas operativos AIX

tsmdlst (Visualizar información sobre dispositivos)

Use el programa de utilidad tsmdlst para ver los nombres del dispositivo y otra información acerca del conmutador de medios y los dispositivos de cinta controlados por el controlador del dispositivo IBM Spectrum Protect.

El programa de utilidad tsmdlst forma parte del paquete de controlador del dispositivo IBM Spectrum Protect que es igual para el servidor y para el agente de almacenamiento. Debe instalar el controlador del dispositivo IBM Spectrum Protect para ejecutar el programa de utilidad tsmdlst para el agente de almacenamiento.

Después de que se configuren los dispositivos, puede ejecutar la herramienta tsmdlst para mostrar la información de dispositivos. La herramienta guarda esta información en archivos que se pueden recuperar. Los archivos se denominan lbinfo para los dispositivos del conmutador de soporte y mtinfo para los dispositivos de cinta. Después de que se añada o se vuelva a configurar un dispositivo, puede actualizar estos archivos ejecutando la herramienta tsmdlst de nuevo.

La herramienta tsmdlst y los archivos de salida que genera se encuentran en el directorio devices/bin, que de forma predeterminada es /opt/tivoli/tsm/devices/bin. Antes de ejecutar la herramienta tsmdlst, asegúrese de que se haya detenido el servidor de IBM Spectrum Protect o que se hayan detenido todas las actividades de los dispositivos. Si un dispositivo está siendo utilizado por el servidor de IBM Spectrum Protect cuando se ejecuta la herramienta tsmdlst, se emite un error de dispositivo ocupado.

Opciones

- /t Muestra los mensajes de rastreo para el programa de utilidad tsmdlst.
- /? Muestra la información de utilización de tsmdlst y sus parámetros.

 Sistemas operativos AIX

Ejemplo: Visualizar información sobre todos los dispositivos

Visualice información sobre todos los dispositivos que ha configurado el controlador de dispositivo de IBM Spectrum Protect:

```
tsmdlst
```

TSM Device Name	Vendor	Product ID	Firmware	World Wide Name	Serial Number
/dev/lb4	ATL	P3000	0100	N/A	1651639999

TSM Device Name	Vendor	Product ID	Firmware	World Wide Name	Serial Number
/dev/mt0	QUANTUM	DLT-S4	2A2A	50:0e:09:e0:00:16:ca:47	QD0619AMD00052
/dev/mt1	QUANTUM	DLT-S4	2A2A	50:0e:09:e0:00:16:cd:e5	QD0624AMD00184
/dev/mt22	QUANTUM	DLT7000	0100	N/A	1651639000
/dev/mt23	QUANTUM	DLT7000	0100	N/A	1651639002

 Sistemas operativos Linux

autoconf (dispositivos de configuración automática)

Utilice el programa de utilidad autoconf para configurar los dispositivos para su uso con el servidor de IBM Spectrum Protect.

La herramienta autoconf realiza las siguientes tareas:

- Carga el controlador en el kernel
- Crea los archivos necesarios para el controlador de dispositivo de IBM Spectrum Protect
- Crea archivos de información de dispositivo para bibliotecas y dispositivos de cinta

La herramienta autoconf se incluye en el paquete de controlador de dispositivo y se instala en el directorio /opt/tivoli/tsm/devices/bin.

Opciones

- a Añade permisos de lectura y grabación a los archivos de dispositivo de IBM Spectrum Protect para permitir a todos los usuarios el acceso a los dispositivos. Especifique este valor para configurar los dispositivos si un usuario no root inicia el servidor de IBM Spectrum Protect.
- g Añade permisos de lectura y grabación a los archivos de dispositivo de IBM Spectrum Protect para permitir que cualquiera que esté en el mismo grupo que un usuario root utilice los dispositivos.
- t Habilita el rastreo de la herramienta autoconf.
- ? Muestra información sobre la herramienta autoconf y sus parámetros.

Ejemplo: Configurar dispositivos utilizando la herramienta autoconf

Ejecute el programa de utilidad autoconf para configurar los dispositivos de IBM Spectrum Protect:

```
> /opt/tivoli/tsm/devices/bin/autoconf
```

 Sistemas operativos Linux

Ejemplo: Para un servidor que se inicia mediante un ID de usuario no root, configurar dispositivos utilizando el programa de utilidad autoconf

Ejecute autoconf para configurar los dispositivos de IBM Spectrum Protect. Utilice la opción a porque el servidor se ha iniciado mediante un ID de usuario que no es el usuario root.

```
> /opt/tivoli/tsm/devices/bin/autoconf -a
```

```
Added the read and write permissions for all users to /dev/sg4.
Added the read and write permissions for all users to /dev/sg5.
Added the read and write permissions for all users to /dev/sg6.
Added the read and write permissions for all users to /dev/sg7.
Added the read and write permissions for all users to /dev/sg8.
Added the read and write permissions for all users to /dev/sg9.
Added the read and write permissions for all users to /dev/sg10.
Added the read and write permissions for all users to /dev/sg11.
Added the read and write permissions for all users to /dev/sg12.
Added the read and write permissions for all users to /dev/sg13.
Added the read and write permissions for all users to /dev/sg14.
Added the read and write permissions for all users to /dev/sg15.
Added the read and write permissions for all users to /dev/sg16.
Added the read and write permissions for all users to /dev/sg17.
Added the read and write permissions for all users to /dev/sg18.
Added the read and write permissions for all users to /dev/sg19.
Added the read and write permissions for all users to /dev/sg20.
Added the read and write permissions for all users to /dev/sg21.
Added the read and write permissions for all users to /dev/sg22.
Added the read and write permissions for all users to /dev/sg23.
Added the read and write permissions for all users to /dev/sg24.
Added the read and write permissions for all users to /dev/sg25.
Added the read and write permissions for all users to /dev/sg26.
Added the read and write permissions for all users to /dev/sg27.
Added the read and write permissions for all users to /dev/sg28.
Added the read and write permissions for all users to /dev/sg29.
```

Tape Drives:

=====


Index	Minor	Host	CHN	ID	LUN	Type	Vendor_ID	Device_Serial_Number	Product_ID	Rev.
000	004	003	000	004	000	001	IBM	1068000439	ULTRIUM-HH5	C5X1
001	007	003	000	008	001	001	HP	01UbWSD-04	Ultrium 2-SCSI	R210
002	008	003	000	008	002	001	HP	01UbWSD-05	Ultrium 2-SCSI	R210
003	010	003	000	008	004	001	HP	01UbWSD-07	Ultrium 3-SCSI	R210
004	012	003	000	008	006	001	HP	01UbWSD-01	Ultrium 3-SCSI	R210

005	013	003	000	008	007	001	HP	01UbWSD-02	Ultrium 3-SCSI	R210
006	014	003	000	008	008	001	HP	01UbWSD-08	Ultrium 3-SCSI	R210
007	015	003	000	008	009	001	HP	01UbWSD-09	Ultrium 3-SCSI	R210
008	016	003	000	008	010	001	HP	01UbWSD-0a	Ultrium 3-SCSI	R210
009	017	003	000	008	011	001	HP	01UbWSD-0b	Ultrium 3-SCSI	R210
010	018	003	000	008	012	001	HP	01UbWSD-0c	Ultrium 3-SCSI	R210
011	019	003	000	008	013	001	HP	01UbWSD-0d	Ultrium 3-SCSI	R210
012	020	003	000	005	000	001	IBM	1068000913	ULTRIUM-HH5	C5X1
013	022	003	000	009	001	001	QUANTUM	01UbWSD-0f	SDLT320	R210
014	023	003	000	009	002	001	QUANTUM	01UbWSD-0g	SDLT320	R210
015	024	003	000	009	003	001	QUANTUM	01UbWSD-0h	SDLT320	R210
016	025	003	000	009	004	001	QUANTUM	01UbWSD-0i	SDLT320	R210
017	026	003	000	006	000	001	IBM	1068001573	ULTRIUM-HH4	B5Q1
018	027	003	000	007	000	001	IBM	1068001545	ULTRIUM-HH4	B5Q1
019	028	003	000	010	000	001	HP	HU19477PAE	Ultrium 5-SCSI	I65W

Medium Changer Devices:

=====

Index	Minor	Host	CHN	ID	LUN	Type	Vendor_ID	Device_Serial_Number	Product_ID	Rev.
000	005	003	000	004	001	008	NEC	2Y11BB0023	LL-2B01	0004
001	006	003	000	008	000	008	HP	01UbWSD-03	VLS	1.00
002	009	003	000	008	003	008	HP	01UbWSD-06	ThinStor AutoLdr	T133
003	011	003	000	008	005	008	HP	01UbWSD-00	ESL E-Series	2.00
004	021	003	000	009	000	008	HP	01UbWSD-0e	MSL6000 Series	0430
005	029	003	000	010	001	008	HP	3615-0101	MSL G3 Series	1120

 Sistemas operativos Windows

tsmdlst (Visualizar información sobre dispositivos)

Utilice el programa de utilidad tsmdlst para ver nombres de dispositivo y otra información sobre el conmutador de soporte o dispositivos de cintas en el sistema.

Opciones

Después de que se configuren los dispositivos, puede ejecutar la herramienta tsmdlst para mostrar la información de dispositivos. El programa de utilizada está en el directorio del servidor de dispositivos, que está en \Program Files\Tivoli\TSM\server por defecto.

`/computer=computer_name`

Especifica el nombre del sistema para el que se enumeran los dispositivos. El valor predeterminado es el sistema local.

`/detail`

Muestra los detalles de los dispositivos en la lista. De manera predeterminada, se muestra un resumen.

`/all`

Muestra información sobre todos los tipos de dispositivos. De manera predeterminada, en los resultados sólo se incluyen las unidades de cinta y las bibliotecas de cinta.

`/nogenerictapecheck`

Omite los pasos para abrir unidades detectadas para ver si son compatibles para el tipo de dispositivo de IBM Spectrum Protect GENERICTAPE.

`/nohbackcheck`

Omite los pasos para la detección de la API del adaptador de bus de host (HBA), que podría acelerar el proceso. Esta opción puede ser útil cuando se necesita depuración.

`/trace`

Se utiliza con fines de diagnóstico. Almacena la salida de rastreo en el archivo tsmdlst_trace.txt.

`/?`

Muestra la información de utilización de tsmdlst y sus parámetros.

`/xinquiry`

Proporciona una forma alternativa para obtener la información del número de serie y del nombre de ámbito mundial. Esta opción sólo se utiliza para los dispositivos que son compatibles con el controlador de dispositivos de cinta de IBM®. Los parámetros siguientes son específicos a la opción `/xinquiry`:

`/processAll`

Indica que el proceso entra en bucle hasta que se procesan todos los dispositivos.

`/maxRetries=#`

Indica el número máximo de intentos para abrir cada unidad. Esta opción requiere la opción `/processAll`.

`/genpathfile`

Utilice esta opción para generar una lista de dispositivos y números de serie. El archivo tsmdlst_pathfile.txt se escribe con información para las opciones `/genmacropathsinc` y `/genmacropathoffline`.

`/includelib`

Si este parámetro se ha especificado con la opción `/genpathfile`, la lista de dispositivos incluye bibliotecas además de unidades.

`/genmacropathsync`

Genera una macro para sincronizar las vías de acceso de IBM Spectrum Protect para el agente de almacenamiento basándose en el número de serie. Una unidad debe tener un número de serie que esté definido en IBM Spectrum Protect para que esta opción funcione.

`/genmacropathoffline`

Genera una macro para actualizar las vías de acceso de IBM Spectrum Protect para el agente de almacenamiento al estado en línea o fuera de línea basándose en la accesibilidad de la unidad. Es posible acceder a una unidad si una llamada abierta de sistema operativo tiene como resultado: `ERROR_SUCCESS`, `ERROR_BUSY` o `ERROR_ACCESS_DENIED`. Esta opción solo funciona para dispositivos que utilizan el controlador de dispositivo de IBM. Para abrir un nombre de dispositivo se precisa un nombre simbólico, por ejemplo, `\\.\tape0`.

Las opciones siguientes solo se utilizan con las opciones `/genmacropathsync` y `/genmacropathoffline`:

`/server=servername`

Especifica el nombre del servidor que utiliza el agente de almacenamiento.

`/stagent=stagentname`

Especifica el nombre del agente de almacenamiento.

`/tcps=address`

Especifica la dirección del servidor de IBM Spectrum Protect.

`/tcpport=port`

Especifica el puerto del servidor de IBM Spectrum Protect. El valor predeterminado es 1500.

`/id=id`

Especifica el identificador administrativo de IBM Spectrum Protect.

`/pass=password`

Especifica la contraseña administrativa de IBM Spectrum Protect.

`/devicetype=drivetype`

Especifica el tipo de dispositivo de la unidad, por ejemplo, `LTO`. Esta opción distingue entre mayúsculas y minúsculas y es opcional.

`/libraryname=libname`

Filtros en el nombre de biblioteca de la unidad, por ejemplo `LTO3584`. Esta opción distingue entre mayúsculas y minúsculas y es opcional.

`/execmacropathsync`

Emite la macro de sincronización de vías de acceso al servidor de IBM Spectrum Protect.

`/execmacropathoffline`

Emite la macro fuera de línea de vías de acceso al servidor de IBM Spectrum Protect.

`/addpaths`

Añade sentencias para definir y actualizar vías de acceso. Esta opción se utiliza con la opción `/genmacropathsync`.

`/verbose`

Lista la información de la unidad y, también, de la vía de acceso devuelta del servidor IBM Spectrum Protect y el contenido del archivo de la vía de acceso.

`/encodednames`

Si una vía de acceso se establece en `online=no`, el nombre de dispositivo codifica la indicación de tiempo, el error y el dispositivo como el nombre del dispositivo actualizado.

Ejemplo: visualizar información sobre dispositivos

Visualizar información sobre dispositivos de cinta y bibliotecas de cintas para un sistema local, WANTON, ejecutando la herramienta `tsmdlst`:

```
tsmdlst
```

El nombre de dispositivo que se visualiza es el nombre de alias que se puede utilizar en el mandato `DEFINE PATH` y el mandato `UPDATE PATH`. El nombre de alias no es el nombre real del dispositivo.

```
Computer Name:      WANTON
OS Version:         6.2
OS Build #:         9200
Controlador de dispositivo de TSM: TSMScsi - No activo
```

```
4 HBAs were detected.
```

Manufacturer	Model	Driver	Version	Firmware	NodeWWN	Description
QLogic Corporation	QLE2562	ql2300.sys	9.1.11.28	7.03.00	20000024FF25F846	QLogic QLE2562 Fibre

```

Channel Adapter
QLogic Corporation QLE2562 ql2300.sys 9.1.11.28 7.03.00 20000024FF25F847 QLogic QLE2562 Fibre
Channel Adapter
QLogic Corporation QLE2562 ql2300.sys 9.1.11.28 7.03.00 20000024FF25F7FE QLogic QLE2562 Fibre
Channel Adapter
QLogic Corporation QLE2562 ql2300.sys 9.1.11.28 7.03.00 20000024FF25F7FF QLogic QLE2562 Fibre
Channel Adapter

```

Nombre	TSM	ID	LUN	Bus	Puerto	SSN	WWN	TSM	Tipo	Controlador	Dispositivo	Identificador
mt0.0.0.7	0	0	0	7		000001327176			5005076300566011	3592	IBM	IBM
03592E06		2883										
lb0.1.0.7	0	1	0	7		0000013400480405			5005076300566011	LIBRARY	IBM	IBM
03584L22		E01q										
mt1.0.0.7	1	0	0	7		000001327147			5005076300566012	3592	IBM	IBM
03592E06		2883										
mt2.0.0.7	2	0	0	7		000001327349			5005076300566013	3592	IBM	IBM
03592E06		2883										
mt3.0.0.7	3	0	0	7		000001327140			5005076300566014	3592	IBM	IBM
03592E06		2883										
mt4.0.0.7	4	0	0	7		1068000254			500507630F51FA05	LTO	IBM	IBM
ULT3580-TD5		D8D4										
lb4.1.0.7	4	1	0	7		0000078216780402			500507630F51FA05	LIBRARY	IBM	IBM
03584L32		C460										
mt5.0.0.7	5	0	0	7		1068000039			500507630F51FA06	LTO	IBM	IBM
ULT3580-TD5		D8D4										
mt6.0.0.7	6	0	0	7		1068000047			500507630F51FA07	LTO	IBM	IBM
ULT3580-TD5		D8D4										
mt7.0.0.7	7	0	0	7		1068000017			500507630F51FA08	LTO	IBM	IBM
ULT3580-TD5		D8D4										

Scripts de servidor y macros para automatización

Puede automatizar tareas administrativas comunes creando scripts de servidor y macros de cliente administrativas de IBM Spectrum Protect. Los scripts de servidor se almacenan en la base de datos del servidor y se pueden planificar para ejecutar con un mandato de planificación administrativa. Las macros de cliente administrativo se almacenan como archivos en el cliente de administración. Las macros no se pueden distribuir entre servidores y no se pueden planificar en el servidor.

- **Scripts de servidor**
Puede automatizar tareas administrativas comunes con scripts que se almacenan en la base de datos del servidor. Puede planificar un script para su proceso mediante el planificador de mandatos de administración en el servidor.
- **Macros de cliente administrativo**
Una macro es un archivo que contiene uno o más mandatos de cliente de administración. Sólo puede ejecutar una macro desde el cliente administrativo en la modalidad de proceso por lotes o en la modalidad interactiva. Las macros se almacenan como archivos en el cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

Scripts de servidor

Puede automatizar tareas administrativas comunes con scripts que se almacenan en la base de datos del servidor. Puede planificar un script para su proceso mediante el planificador de mandatos de administración en el servidor.

Los scripts de IBM Spectrum Protect admiten las siguientes prestaciones y sentencias:

- Sustitución de parámetros de mandatos.
- Mandatos SELECT que se especifican al procesar el script.
- Control de la ejecución de mandatos, como las opciones de proceso PARALLEL y SERIAL.
- Sentencias de flujo lógico condicional. Estas sentencias de flujo lógicas incluyen las siguientes sentencias:
 - La cláusula IF; esta cláusula determina cómo debe continuar el proceso en función del valor del código de retorno actual.
 - La sentencia EXIT; esta sentencia finaliza el proceso del script.
 - Las sentencias GOTO y LABEL. Estas sentencias indican que el flujo lógico continúa el proceso con la línea que empieza por la etiqueta especificada.
- Línea de comentarios.

Se proporcionan scripts de ejemplo en el archivo scripts.smp. Los scripts de ejemplo tienen un orden de ejecución de ejemplo para la planificación de mandatos de administración.

Si uno de los mandatos especificados en el script no se procesa correctamente, los demás mandatos no se procesan.

- Definición de un script de servidor
Se puede definir un script de servidor línea a línea, crear un archivo que contenga las líneas de mandatos o copiar un script ya existente.
- Actualización de un script
Puede actualizar un script para cambiar una línea de mandatos o para añadir una línea de mandatos a un script.
- Consulta de un script de servidor para crear otro script de servidor
Se pueden crear más scripts de servidor consultando un script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene se puede utilizar como entrada de otro script sin tener que crear un script línea a línea.
- Ejecución de un script del servidor
Para procesar un script, emita el mandato RUN. Se puede ejecutar un script que contenga variables de sustitución especificándolas junto con el mandato RUN.

Definición de un script de servidor

Se puede definir un script de servidor línea a línea, crear un archivo que contenga las líneas de mandatos o copiar un script ya existente.

Acerca de esta tarea

Restricción: No se puede redirigir la salida de un mandato dentro de un script de servidor. En su lugar, ejecute el script y, a continuación, especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

Procedimiento

1. Defina un script con el mandato DEFINE SCRIPT. Se puede definir inicialmente la primera línea del script con este mandato. Por ejemplo:

```
define script qaixc "select node_name from nodes where platform='aix'"
desc='Visualizar clientes AIX'
```

En este ejemplo se define el script como QAIXC. Al ejecutar el script, se visualizan todos los clientes AIX.

2. Defina más líneas en el script con el mandato UPDATE SCRIPT. Por ejemplo, para añadir un mandato QUERY SESSION, entre:

```
update script qaixc "query session *"
```

3. Opcional: Puede especificar un parámetro WAIT con el mandato DEFINE CLIENTACTION. Utilizando este parámetro, puede especificar que la acción del cliente se debe completar antes de que se procese el paso siguiente en el script de mandato o la macro.
 4. Opcional: Para ayudarle a determinar cuándo hay un problema en un mandato en un script, utilice el mandato ISSUE MESSAGE.
- Ejecución de mandatos en paralelo o en serie
Tiene la posibilidad de ejecutar mandatos en serie, en paralelo o en serie y en paralelo. También puede hacerlo utilizando los mandatos de script SERIAL o PARALLEL del parámetro COMMAND_LINE de DEFINE y UPDATE SCRIPT. Por lo tanto, es posible ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente.
 - Continuación de mandatos a través de varias líneas de mandatos
Los mandatos largos se pueden continuar en varias líneas de mandatos especificando el carácter de continuación (-) como el último carácter de un mandato que continúa.
 - Inclusión de las variables de sustitución en un script
En un script se pueden incluir variables de sustitución. Las variables de sustitución se especifican con el carácter \$ seguido de un número que representa la posición del parámetro al procesarse el script.
 - Inclusión de sentencias de flujo lógico en un script
Se pueden utilizar sentencias de flujo lógico condicional en función de los códigos de retorno emitidos en el proceso de mandatos anterior. Utilizando estas sentencias lógicas, puede procesar los scripts según el resultado de ciertos mandatos. Se pueden utilizar las sentencias IF, EXIT, o GOTO (etiqueta).
 - Utilización de mandatos SELECT en un script
Un script de IBM Spectrum Protect es uno o varios mandatos almacenados como un objeto en la base de datos. Puede definir un script que contenga uno o más mandatos SELECT.

Ejecución de mandatos en paralelo o en serie

Tiene la posibilidad de ejecutar mandatos en serie, en paralelo o en serie y en paralelo. También puede hacerlo utilizando los mandatos de script SERIAL o PARALLEL del parámetro COMMAND_LINE de DEFINE y UPDATE SCRIPT. Por lo tanto, es posible ejecutar varios

mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente.

Acerca de esta tarea

La ejecución de mandatos en serie en un script garantiza que cualquier mandato precedente haya finalizado antes de continuar y garantiza que los mandatos siguientes se ejecuten en serie. Cuando se inicia un script, todos los mandatos se ejecutan en serie hasta que aparece un mandato PARALLEL. Varios mandatos que se ejecutan en paralelo y que acceden a recursos comunes, como las unidades de cintas, pueden ejecutarse en serie.

Los códigos de retorno de script siguen siendo los mismos antes y después de que se ejecute un mandato PARALLEL. Cuando aparece un mandato SERIAL, el código de retorno de script se establece en el código de retorno máximo de todos los mandatos anteriores ejecutados en paralelo.

Al utilizar mandatos de servidor que admiten el parámetro WAIT después de un mandato PARALLEL, el comportamiento es el siguiente:

- Si especifica (o utiliza el valor predeterminado) WAIT=NO, un script no espera hasta la finalización del mandato cuando aparece un mandato SERIAL posterior. El código de retorno de dicho mandato refleja el proceso sólo hasta el punto en el que el mandato inicia un proceso subordinado. El código de retorno final del mandato no está disponible para el script.
- Si especifica WAIT=YES, su script espera hasta la finalización del mandato cuando aparece un mandato SERIAL posterior. El código de retorno de dicho mandato refleja el proceso de todo el mandato.

En la mayoría de los casos, puede utilizar WAIT=YES en los mandatos que se ejecutan en paralelo.

Restricción: Si el mandato inicia un proceso en segundo plano que no tiene el parámetro WAIT, el mandato se considera completado después de que se inicie la hebra de fondo. Por lo tanto, el mandato sólo puede ejecutarse en paralelo.

El ejemplo siguiente ilustra el modo en que se utiliza el mandato PARALLEL para realizar una copia de seguridad, migrar y reclamar agrupaciones de almacenamiento.

```
/*run multiple commands in parallel and wait for
them to complete before proceeding*/
PARALLEL
/*back up four storage pools simultaneously*/
BACKUP STGPOOL PRIMPOOL1 COPYPOOL1 WAIT=YES
BACKUP STGPOOL PRIMPOOL2 COPYPOOL2 WAIT=YES
BACKUP STGPOOL PRIMPOOL3 COPYPOOL3 WAIT=YES
BACKUP STGPOOL PRIMPOOL4 COPYPOOL4 WAIT=YES
/*wait for all previous commands to finish*/
SERIAL
/*after the backups complete, migrate stgpools
simultaneously*/
PARALLEL
MIGRATE STGPOOL PRIMPOOL1 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL2 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL3 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL4 DURATION=90 WAIT=YES
/*wait for all previous commands to finish*/
SERIAL
/*after migration completes, reclaim storage
pools simultaneously*/
PARALLEL
RECLAIM STGPOOL PRIMPOOL1 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL2 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL3 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL4 DURATION=120 WAIT=YES
```

Referencia relacionada:

DEFINE SCRIPT (definir un script de servidor)
UPDATE SCRIPT (actualizar un script de servidor)

Continuación de mandatos a través de varias líneas de mandatos

Los mandatos largos se pueden continuar en varias líneas de mandatos especificando el carácter de continuación (-) como el último carácter de un mandato que continúa.

Acerca de esta tarea

En el ejemplo siguiente se continúa una sentencia SQL en varias líneas de mandatos:

```

/*-----*/
/* Ejemplo de continuación      */
SELECT-
* FROM-
NODE WHERE-
PLATFORM='win32'

```

Cuando se procesa este mandato, se ejecuta el siguiente mandato:

```
select * from nodes where platform='win32'
```

Inclusión de las variables de sustitución en un script

En un script se pueden incluir variables de sustitución. Las variables de sustitución se especifican con el carácter \$ seguido de un número que representa la posición del parámetro al procesarse el script.

Acerca de esta tarea

En el ejemplo siguiente, el script SQLSAMPLE especifica las variables de sustitución \$1 y \$2:

```

/*-----*/
/* Ejemplo de sustitución      */
/* -----*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'

```

Al ejecutar el script, debe especificar dos valores, uno para \$1 y otro para \$2. Por ejemplo:

```
run sqlsample
nombre_nodo aix
```

El mandato que se procesa cuando se ejecuta el script SQLSAMPLE es el siguiente:

```
select nombre_nodo from nodes where
platform='aix'
```

Inclusión de sentencias de flujo lógico en un script

Se pueden utilizar sentencias de flujo lógico condicional en función de los códigos de retorno emitidos en el proceso de mandatos anterior. Utilizando estas sentencias lógicas, puede procesar los scripts según el resultado de ciertos mandatos. Se pueden utilizar las sentencias IF, EXIT, o GOTO (etiqueta).

A medida que cada mandato se procesa en un script, el código de retorno se guarda para su posible evaluación antes de procesarse el siguiente mandato. El código de retorno puede ser de tres clases de gravedad: OK (correcto), WARNING (aviso) o ERROR (error). Consulte Códigos de devolución para utilizar en scripts para obtener una lista de códigos de devolución válidos y niveles de gravedad.

- Especificación de la cláusula IF
La cláusula IF se puede utilizar al principio de una línea de mandatos para determinar cómo debe continuar el proceso del script en función del valor de código de retorno actual. En la cláusula IF se especifica la gravedad o el valor simbólico del código de retorno.
- Especificación de la sentencia EXIT
Utilice la sentencia EXIT para finalizar un proceso de script.
- Especificación de la sentencia GOTO
La sentencia GOTO se utiliza conjuntamente con una sentencia de etiqueta. La sentencia de etiqueta es el destino de la sentencia GOTO. La sentencia GOTO dirige el proceso del script a la línea que contiene la sentencia de etiqueta para que el proceso se reanude desde ese punto.

Especificación de la cláusula IF

La cláusula IF se puede utilizar al principio de una línea de mandatos para determinar cómo debe continuar el proceso del script en función del valor de código de retorno actual. En la cláusula IF se especifica la gravedad o el valor simbólico del código de retorno.

Acerca de esta tarea

El servidor establece inicialmente el código de retorno al principio del script en RC_OK. Cada mandato procesado actualiza el código de retorno. Si el código de retorno actual del mandato procesado es igual que alguno de los códigos de retorno o gravedades que hay en la cláusula IF, se procesará el resto de la línea. Si el código de retorno actual es distinto de uno de los valores listados, se salta la línea.

En el ejemplo siguiente de script, se hace una copia de seguridad de la agrupación de almacenamiento BACKUPPOOL sólo si no hay ninguna sesión que esté accediendo al servidor en la actualidad. La copia de seguridad continúa sólo si se recibe el código de retorno RC_NOTFOUND:

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* No hay sesiones si se recibe rc_notfound */
if(rc_notfound) backup stg backuppool copypool
```

En el ejemplo siguiente de script, se hace una copia de seguridad de la agrupación de almacenamiento BACKUPPOOL si se detecta un código de retorno con gravedad de aviso:

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* No hay sesiones si se recibe rc_notfound */
if(warning) backup stg backuppool copypool
```

Especificación de la sentencia EXIT

Utilice la sentencia EXIT para finalizar un proceso de script.

Acerca de esta tarea

En el ejemplo siguiente, se utiliza la cláusula IF junto con RC_OK para determinar si los clientes están accediendo al servidor. Si se recibe un código de retorno RC_OK, indica que las sesiones de cliente están accediendo al servidor. El script continúa con la sentencia exit y no se inicia la copia de seguridad.

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* Hay sesiones si se recibe rc_ok */
if(rc_ok) exit
backup stg backuppool copypool
```

Especificación de la sentencia GOTO

La sentencia GOTO se utiliza conjuntamente con una sentencia de etiqueta. La sentencia de etiqueta es el destino de la sentencia GOTO. La sentencia GOTO dirige el proceso del script a la línea que contiene la sentencia de etiqueta para que el proceso se reanude desde ese punto.

Acerca de esta tarea

La sentencia de etiqueta siempre va seguida de dos puntos (:) y puede tener un espacio en blanco después de los dos puntos. En el ejemplo siguiente, se utiliza la sentencia GOTO para hacer una copia de seguridad de la agrupación de almacenamiento sólo si no hay ninguna sesión que esté accediendo al servidor en la actualidad. En este ejemplo, el código de retorno RC_OK indica que hay clientes accediendo al servidor. La sentencia GOTO dirige el proceso a la etiqueta done: que contiene la sentencia EXIT que finaliza el proceso del script:

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* Hay sesiones si se recibe rc_ok */
if(rc_ok) goto done
backup stg backuppool copypool
done:exit
```

Utilización de mandatos SELECT en un script

Un script de IBM Spectrum Protect es uno o varios mandatos almacenados como un objeto en la base de datos. Puede definir un script que contenga uno o más mandatos SELECT.

Acerca de esta tarea

Un script puede ejecutarse desde un cliente de administración o la consola del servidor. También lo puede incluir como una planificación de mandatos de administración para que se ejecuten automáticamente. Consulte el apartado Scripts de servidor para obtener más detalles.

IBM Spectrum Protect se distribuye con un archivo que contiene diversos scripts a modo de ejemplo. El archivo, `scripts.smp`, se encuentra en el directorio del servidor. Para crear y guardar los scripts como objetos en la base de datos del servidor, emita el mandato `DSMSERV RUNFILE` durante la instalación:

```
> dsmserv runfile scripts.smp
```

También puede ejecutar el archivo como una macro desde un cliente de línea de mandatos de administración:

```
macro scripts.smp
```

El archivo de scripts de ejemplo contiene mandatos. Estos mandatos suprimen los scripts que tienen los mismos nombres que los que se van a definir y, a continuación, definen los scripts. La mayor parte de los ejemplos crean mandatos `SELECT`, pero otros llevan a cabo otras tareas tales como hacer copias de seguridad de agrupaciones de almacenamiento. También puede copiar y modificar el archivo de scripts de ejemplo para crear sus propios scripts.

A continuación se incluyen algunos ejemplos del archivo de scripts de ejemplo:

```
def script q_inactive_days /* -----*/
upd script q_inactive_days /* Nombre de script:  Q_INACTIVE          */
upd script q_inactive_days /* Descripción: Muestra nodos que no han   */
upd script q_inactive_days /* accedido al servidor de seguridad durante */
upd script q_inactive_days /* un número especificado de días      */
upd script q_inactive_days /* Parámetro 1: días                */
upd script q_inactive_days /* Ejemplo:      run q_inactive_days 5      */
upd script q_inactive_days /* -----*/
upd script q_inactive_days "select node_name,lastacc_time from nodes where -"
upd script q_inactive_days " cast((current_timestamp-lastacc_time)days as -"
upd script q_inactive_days " decimal) >= $1 "

/* Muestra mensajes en las anotaciones de actividades de gravedad X o Y          */

def script q_msg_sev desc='Muestra mensajes en las anotaciones de gravedad X o Y'
upd script q_msg_sev /* -----*/
upd script q_msg_sev /* Nombre de script:  Q_MSG_SEV          */
upd script q_msg_sev /* Descripción: Muestra mensajes en las   */
upd script q_msg_sev /* anotaciones de actividades con una    */
upd script q_msg_sev /* de las gravedades especificadas.     */
upd script q_msg_sev /* Parámetro 1: gravedad 1              */
upd script q_msg_sev /* Parámetro 2: gravedad 2              */
upd script q_msg_sev /* donde la gravedad es I, W, E, S, o D  */
upd script q_msg_sev /* Ejemplo:  ejecute q_msg_sev S E      */
upd script q_msg_sev /* -----*/
upd script q_msg_sev "select date_time,msgno,message from actlog -"
upd script q_msg_sev " where severity=upper('$1') or severity=upper('$2')"
```

Actualización de un script

Puede actualizar un script para cambiar una línea de mandatos o para añadir una línea de mandatos a un script.

- Añadir un nuevo mandato
Para agregar una línea de mandatos a un script ya existente, emita el mandato `UPDATE SCRIPT` sin el parámetro `LINE=`. La línea de mandatos agregada recibe un número de línea de cinco unidades más que el último número de línea de mandatos de la secuencia de líneas de mandatos. Por ejemplo, si el script acaba con la línea `010`, a la línea de mandatos agregada se le asigna el número de línea `015`.
- Sustitución de un mandato existente
Puede cambiar una línea de mandatos existente especificando el parámetro `LINE=`.
- Adición de un mandato y un número de línea
Puede cambiar un script existente añadiendo líneas nuevas.
- Supresión de un mandato de un script del servidor
Se puede suprimir una línea de mandatos concreta de un script. Al especificar un número de línea, sólo se suprime del script la línea de mandatos correspondiente.

Añadir un nuevo mandato

Para agregar una línea de mandatos a un script ya existente, emita el mandato UPDATE SCRIPT sin el parámetro LINE=. La línea de mandatos agregada recibe un número de línea de cinco unidades más que el último número de línea de mandatos de la secuencia de líneas de mandatos. Por ejemplo, si el script acaba con la línea 010, a la línea de mandatos agregada se le asigna el número de línea 015.

Acerca de esta tarea

A continuación, se presenta un ejemplo del script QSTATUS. El script tiene las líneas 001, 005 y 010 según se indica:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
```

Para añadir el mandato QUERY SESSION al final del script, emita el mandato siguiente:

```
update script qstatus "query session"
```

El mandato QUERY SESSION recibe el número de línea de mandatos 015 y el script actualizado queda del siguiente modo:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION
```

Sustitución de un mandato existente

Puede cambiar una línea de mandatos existente especificando el parámetro LINE=.

Acerca de esta tarea

El número de línea 010 del script QSTATUS contiene un mandato QUERY PROCESS. Para sustituir el mandato QUERY PROCESS por el mandato QUERY STGPOOL, especifique el parámetro LINE= según se indica:

```
update script qstatus "query stgpool" line=10
```

El script QSTATUS se actualiza para contener las líneas siguientes:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY STGPOOL
015 QUERY SESSION
```

Adición de un mandato y un número de línea

Puede cambiar un script existente añadiendo líneas nuevas.

Acerca de esta tarea

Para añadir el mandato QUERY NODE como la nueva línea 007 del script QSTATUS, emita el mandato siguiente:

```
update script qstatus "query node" line=7
```

El script QSTATUS se actualiza para contener las líneas siguientes:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION
```

Supresión de un mandato de un script del servidor

Se puede suprimir una línea de mandatos concreta de un script. Al especificar un número de línea, sólo se suprime del script la línea de mandatos correspondiente.

Acerca de esta tarea

Por ejemplo, para suprimir la línea de mandatos 007 del script QSTATUS, emita el mandato siguiente:

```
delete script qstatus line=7
```

Consulta de un script de servidor para crear otro script de servidor

Se pueden crear más scripts de servidor consultando un script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene se puede utilizar como entrada de otro script sin tener que crear un script línea a línea.

Acerca de esta tarea

El ejemplo siguiente muestra cómo consultar el script SRTL2 y dirigir la salida a newscript.script:

```
query script srtl2 format=raw outputfile=newscript.script
```

A continuación, puede editar el archivo newscript.script con un editor del que disponga el sistema. Para crear un nuevo script utilizando la salida editada de la consulta, emita:

```
define script srtnew file=newscript.script
```

Ejecución de un script del servidor

Para procesar un script, emita el mandato RUN. Se puede ejecutar un script que contenga variables de sustitución especificándolas junto con el mandato RUN.

Acerca de esta tarea

Para detener el script que se está ejecutando, el administrador deberá parar el servidor. No puede cancelar un script después de iniciarlo utilizando un mandato de IBM Spectrum Protect.

Procedimiento

- Obtenga una vista previa de los mandatos de un script para evaluar este antes de ejecutarlo. Para previsualizar el script sin ejecutar los mandatos, escriba el mandato RUN con el parámetro PREVIEW=YES. Si el script contiene variables de sustitución, los mandatos se muestran con las variables sustituidas.
- Ejecute un mandato que no tenga ninguna variable especificando el siguiente mandato: `run qaixc` donde `qaixc` es el nombre del script.
- Ejecute un script que contenga variables de sustitución especificando los valores variables con el mandato. Contenido del script:

```
/*-----*/  
/* Ejemplo de continuación y sustitución      */  
/* -----*/  
SELECT-  
$1 FROM-  
NODES WHERE-  
PLATFORM='$2'
```

Para ejecutar este script, introduzca el siguiente mandato:

```
run qaixc nombre_nodo aix
```

Donde `node_name` es el valor de la variable `$1` y `aix` es el valor de la variable `$2`.

Referencia relacionada:

RUN (ejecutar un script de servidor)

Macros de cliente administrativo

Una macro es un archivo que contiene uno o más mandatos de cliente de administración. Sólo puede ejecutar una macro desde el cliente administrativo en la modalidad de proceso por lotes o en la modalidad interactiva. Las macros se almacenan como archivos en el cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

Las macros pueden incluir los elementos siguientes:

- mandatos de servidor administrativo
- Comentarios.

- Caracteres de continuación.
- Variables.

El nombre de una macro debe ajustarse a los convenios de denominación del cliente de administración que ejecuta el sistema operativo.

En una macro que contenga varios mandatos, utilice los mandatos COMMIT y ROLLBACK para controlar el proceso de los mandatos en la macro.

Puede incluir el mandato MACRO dentro de un archivo de macros para llamar a otras macros, hasta un máximo de 10 niveles de profundidad. La macro a la que se llama desde la línea de mandatos del cliente de administración se denomina macro de nivel superior. Las macros a las que se llama desde dentro de la macro de nivel superior se denominan macros *anidadas*.

- Grabación de mandatos en una macro
Añada mandatos administrativos a una macro. El cliente de administración no tiene en cuenta las líneas en blanco que contiene la macro. No obstante, una línea completamente en blanco termina un mandato continuo (con un carácter de continuación).
- Grabación de comentarios en una macro
Añada comentarios al archivo de macro para describir la finalidad o los mandatos incluidos en él.
- Inclusión de caracteres de continuación en una macro
Puede utilizar caracteres de continuación en un archivo de macro cuando desee ejecutar un mandato que sea más largo que el ancho de la pantalla o de la ventana.
- Inclusión de las variables de sustitución en un macro
Puede utilizar variables de sustitución en una macro para que, al ejecutar la macro, pueda proporcionar valores para elementos como parámetros de mandato. Al emplear variables de sustitución, puede utilizar una macro una y otra vez, siempre que necesite llevar a cabo la misma tarea para objetos distintos o con valores de parámetros diferentes.
- Ejecución de una macro
Utilice el mandato MACRO cuando desee ejecutar una macro. Puede entrar el mandato MACRO en la modalidad de proceso por lotes o en la modalidad interactiva.
- Proceso de mandatos en una macro
Cuando emita un mandato MACRO, el servidor procesa todos los mandatos del archivo de macros por orden, incluidos los mandatos que están contenidos en las macros anidadas. El servidor compromete todos los mandatos de una macro una vez finalizado correctamente el proceso de la macro de nivel superior.

Grabación de mandatos en una macro

Añada mandatos administrativos a una macro. El cliente de administración no tiene en cuenta las líneas en blanco que contiene la macro. No obstante, una línea completamente en blanco termina un mandato continuo (con un carácter de continuación).

Acerca de esta tarea

A continuación figura un ejemplo de una macro denominada REG.MAC que registra un nuevo administrador y le concede autorización:

```
register admin pease mypasswd -
  contact='david pease, x1234'
grant authority pease -
  classes=policy,storage -
  domains=domain1, domain2 -
  stgpools=stgpool1, stgpool2
```

Este ejemplo utiliza caracteres de continuación en el archivo de macros. Para obtener más información acerca de los caracteres de continuación, consulte el apartado Inclusión de caracteres de continuación en una macro.

Una vez creado un archivo de macros, puede actualizar la información que contiene el mismo y volver a utilizarlo. También puede copiar el archivo de macro. Después de copiar un archivo de macro, puede modificar y ejecutar la copia.

Grabación de comentarios en una macro

Añada comentarios al archivo de macro para describir la finalidad o los mandatos incluidos en él.

Acerca de esta tarea

Para escribir un comentario:

- Escriba una barra inclinada y un asterisco (/*) para indicar el principio del comentario.
- Escriba el comentario.

- Escriba un asterisco y una barra inclinada (*) para indicar el final del comentario.

Puede escribir un comentario en una línea dedicada únicamente a comentarios o colocarlo en una línea que contiene un mandato o parte de un mandato.

Por ejemplo, para utilizar un comentario para identificar la finalidad de una macro, escriba la línea siguiente:

```
/* auth.mac-inscribir nuevos nodos */
```

O puede escribir un comentario para explicar algo acerca de un mandato o parte de un mandato:

```
domain=domain1          /* asignar nodo a domain1 */
```

Los comentarios no pueden anidarse y no pueden fragmentar líneas. Cada línea de un comentario debe contener los delimitadores de comentarios.

Inclusión de caracteres de continuación en una macro

Puede utilizar caracteres de continuación en un archivo de macro cuando desee ejecutar un mandato que sea más largo que el ancho de la pantalla o de la ventana.

Acerca de esta tarea

Sin caracteres de continuación, puede especificar hasta 256 caracteres. Con los caracteres de continuación, este límite se amplía a 1500 caracteres. En el mandato MACRO, los valores de las variables de sustitución se incluyen en el recuento de caracteres.

Para utilizar un carácter de continuación, entre un guión o una barra inclinada invertida al final de la línea que desea a continuación. Con los caracteres de continuación, puede continuar las líneas siguientes de una macro.

Ejemplos

- Continúe un mandato, por ejemplo:

```
register admin pease mypasswd -  
contact="david, ext1234"
```

- Continúe una lista de valores especificando un guión o una barra inclinada invertida, sin ningún espacio en blanco precedente, después de la última coma de la lista que especifique en la primera línea. A continuación, entre los elementos de la lista restantes en la línea siguiente sin anteponer ningún espacio en blanco. En el ejemplo siguiente, una lista de nombres de agrupación de almacenamiento continúa entre líneas:

```
stgpools=stg1, stg2, stg3, -  
stg4, stg5, stg6
```

- Continúe una serie de valores que está especificada entre comillas entrando la primera parte de la serie entre comillas, seguida por un guión o una barra inclinada invertida al final de la línea. A continuación, entre el resto de la serie en la línea siguiente. Cierre el resto de la serie en el mismo tipo de comillas. El ejemplo siguiente muestra una serie que continúa entre líneas:

```
contact="david pease, bldg. 100, room 2b, san jose, "-  
"ext. 1234, alternate contact-norm pass, ext 2345"
```

Las dos series se concatenan sin ningún espacio en blanco. Debe utilizar este método sólo para continuar una serie de valores entre comillas en más de una línea.

Inclusión de las variables de sustitución en un macro

Puede utilizar variables de sustitución en una macro para que, al ejecutar la macro, pueda proporcionar valores para elementos como parámetros de mandato. Al emplear variables de sustitución, puede utilizar una macro una y otra vez, siempre que necesite llevar a cabo la misma tarea para objetos distintos o con valores de parámetros diferentes.

Acerca de esta tarea

Una variable de sustitución consta de un signo de porcentaje (%), seguido de un número exclusivo que identifica la variable de sustitución. Cuando ejecute el archivo con el mandato MACRO, debe especificar los valores de las variables.

Restricciones:

- Si el sistema utiliza el signo de porcentaje como carácter comodín, el cliente administrativo interpreta una expresión coincidente con el patrón de una macro en que el signo de porcentaje va inmediatamente seguido de un dígito numérico como variable de sustitución.
- Las variables de sustitución no se pueden delimitar mediante comillas. Sin embargo, un valor proporcionado como sustitución de la variable puede ser una serie entrecomillada.

Ejemplo

Cree una macro denominada AUTH.MAC para registrar nodos nuevos. La macro tiene cuatro variables de sustitución para parámetros en el mandato:

```
/* inscribir nuevos nodos */
register node %1 %2 -      /* contraseña de ID de usuario      */
  contact=%3 -           /* 'nombre, número teléfono' */
  domain=%4              /* dominio de políticas      */
```

Cuando ejecute la macro, debe entrar los valores que desea pasar al servidor para procesar el mandato.

Por ejemplo, para utilizar la macro para registrar el nodo denominado DAVID con una contraseña de DAVIDPW, incluir el nombre y el número de teléfono como información de contacto y asignarlo al dominio de políticas DOMAIN1, entre el siguiente mandato:

```
macro auth.mac david davidpw "david pease, x1234" domain1
```

Ejecución de una macro

Utilice el mandato MACRO cuando desee ejecutar una macro. Puede entrar el mandato MACRO en la modalidad de proceso por lotes o en la modalidad interactiva.

Acerca de esta tarea

Si la macro no contiene variables de sustitución, ejecute la macro especificando el mandato MACRO con el nombre del archivo de macro. Por ejemplo:

```
macro reg.mac
```

Si la macro contiene variables de sustitución, incluya los valores que desea suministrar tras el nombre de la macro. Los distintos valores se delimitan mediante un espacio. Por ejemplo:

```
macro auth.mac pease mypasswd "david pease, x1234" domain1
```

Si el número de valores que especifica es inferior al de variables de sustitución que hay en la macro, el cliente de administración sustituye las variables restantes por series nulas.

Si desea omitir uno o más valores entre los valores, especifique una cadena nula ("") para cada uno de los valores omitidos. Por ejemplo, para omitir la información de contacto en el ejemplo anterior, escriba:

```
macro auth.mac pease mypasswd "" domain1
```

Referencia relacionada:

MACRO (Invocar una macro)

Proceso de mandatos en una macro

Cuando emita un mandato MACRO, el servidor procesa todos los mandatos del archivo de macros por orden, incluidos los mandatos que están contenidos en las macros anidadas. El servidor compromete todos los mandatos de una macro una vez finalizado correctamente el proceso de la macro de nivel superior.

Si se produce un error en algún mandato de la macro o de alguna de las macros anidadas, el servidor termina el proceso y retrotrae los cambios originados por todos los mandatos anteriores.

Si especifica la opción ITEMCOMMIT al introducir el mandato DSMADMC, el servidor compromete uno a uno cada uno de los mandatos en un script o en una macro, una vez finalizado correctamente el proceso de cada uno de ellos. Si se produce algún error, el servidor continúa con el proceso y sólo retrotrae los cambios provocados por el mandato erróneo.

Puede controlar con precisión cuándo se comprometen los mandatos con el mandato COMMIT. Si se produce un error al procesar los mandatos de una macro, el servidor termina el proceso de la macro y retrotrae los cambios no comprometidos. Los cambios no

comprometidos son los mandatos que se han procesado desde el último mandato COMMIT. Asegúrese de que la sesión del cliente de administración no se esté ejecutando con la opción ITEMCOMMIT si desea controlar el proceso de mandatos con el mandato COMMIT.

Puede probar una macro antes de implementarla mediante el mandato ROLLBACK. Puede introducir los mandatos (excepto el mandato COMMIT) que desea emitir en la macro e introducir ROLLBACK como último mandato. A continuación, puede ejecutar la macro para verificar que todos los mandatos se procesen correctamente. El mandato ROLLBACK que ha incluido al final retrotrae los cambios efectuados en la base de datos como consecuencia de los mandatos. No olvide eliminar el mandato ROLLBACK antes de poner la macro a disposición para su uso real. Asimismo, compruebe que la sesión del cliente de administración no se esté ejecutando con la opción ITEMCOMMIT si desea controlar el proceso de mandatos con el mandato ROLLBACK.

Consejo: Los mandatos que inician procesos de fondo no pueden retrotraerse.

Si tiene una serie de mandatos que se procesan correctamente en la línea de mandatos pero no al emitirse dentro de una macro, es probable que existan dependencias entre los mandatos. Puede suceder que un mandato emitido dentro de una macro no pueda procesarse correctamente hasta que se haya comprometido un mandato anterior emitido dentro de la misma macro. Lleve a cabo alguna de las acciones siguientes para que estos mandatos se procesen correctamente dentro de una macro:

- Inserte un mandato COMMIT antes del mandato que depende de un mandato anterior. Por ejemplo, si COMMAND C depende de COMMAND B, inserte un mandato COMMIT antes de COMMAND C.

```
command a
command b
commit
command c/
```

- Inicie la sesión del cliente de administración utilizando la opción ITEMCOMMIT. Esta opción hace que todos los mandatos de una macro se confirmen antes de que se procese el mandato siguiente.

Referencia relacionada:

COMMIT (controlar la validación de mandatos en una macro)

ROLLBACK (Retrotraer cambios no validados en una macro)

Códigos de retorno de los scripts para IBM Spectrum Protect

Puede escribir scripts de IBM Spectrum Protect que utilizan códigos de retorno para determinar cómo continúa el proceso de script. Los códigos de retorno pueden ser de una de estas tres gravedades: OK, WARNING, ERROR.

Los scripts de IBM Spectrum Protect utilizan el código de retorno simbólico para el procesamiento, no el valor numérico. El cliente de administración muestra los valores numéricos cuando se ejecuta un mandato. Los códigos de retorno se muestran en la tabla siguiente.

Tabla 1. Códigos de retorno

Código de retorno	Gravedad	Valor numérico	Descripción
RC_OK	Aceptar	0	El mandato se ha completado satisfactoriamente.
RC_UNKNOWN	ERROR	2	El mandato no se a encontrado; no se reconoce el mandato.
RC_SYNTAX	ERROR	3	El mandato es válido, pero uno o más parámetros no se han especificado correctamente.
RC_ERROR	ERROR	4	Un error interno ha impedido que el mandato se completara correctamente.
RC_NOMEMORY	ERROR	5	El mandato no se ha podido completar porque no hay memoria suficiente en el servidor.
RC_NOLOG	ERROR	6	El mandato no se ha podido completar porque no hay espacio de registro de recuperación suficiente en el servidor.
RC_NODB	ERROR	7	El mandato no se puede completar porque no hay espacio de base de datos suficiente en el servidor.
RC_NOSTORAGE	ERROR	8	El mandato no se puede completar porque no hay espacio de almacenamiento suficiente en el servidor.
RC_NOAUTH	ERROR	9	El mandato ha fallado porque el administrador no está autorizado para emitir este mandato.

Código de retorno	Gravedad	Valor numérico	Descripción
RC_EXISTS	ERROR	10	El mandato ha fallado porque el objeto especificado ya existe en el servidor.
RC_NOTFOUND	AVISO	11	Devuelto por un mandato QUERY o SQL SELECT cuando no se encuentran objetos que coincidan con las especificaciones.
RC_INUSE	ERROR	12	El mandato ha fallado porque el objeto con el que se va a operar estaba en uso.
RC_ISREFERENCED	ERROR	13	El mandato ha fallado porque el objeto en el que se iba a operar todavía está siendo referenciado por otro servidor en construcción.
RC_NOTAVAILABLE	ERROR	14	El mandato ha fallado porque el objeto con el que se va a operar no está disponible.
RC_IOERROR	ERROR	15	El mandato ha fallado porque ha encontrado un error de entrada/salida (E/S) en el servidor.
RC_NOTXN	ERROR	16	El mandato ha fallado porque la transacción de una base de datos ha fallado en el servidor.
RC_NOLOCK	ERROR	17	El mandato ha fallado porque se ha producido un conflicto de bloqueo en la base de datos del servidor.
RC_NOTHREAD	ERROR	19	El mandato no se ha podido completar porque no hay memoria suficiente en el servidor.
RC_LICENSE	ERROR	20	El mandato ha fallado porque el servidor no cumple con la licencia.
RC_INVDEST	ERROR	21	El mandato ha fallado porque el valor de destino no es válido.
RC_IFILEOPEN	ERROR	22	El mandato ha fallado porque el archivo de entrada necesario no se ha podido abrir.
RC_OFILEOPEN	ERROR	23	El mandato ha fallado porque no ha podido abrir el archivo de salida necesario.
RC_OFILEWRITE	ERROR	24	El mandato ha fallado porque no ha podido grabarse correctamente en un archivo de salida necesario.
RC_INVADMIN	ERROR	25	El mandato falló porque el administrador no se había definido.
RC_SQLERROR	ERROR	26	Se ha detectado un error de SQL durante la consulta de sentencia SELECT.
RC_INVALIDUSE	ERROR	27	El mandato ha fallado porque se ha emitido de manera no válida.
RC_NOTABLE	ERROR	28	El mandato ha fallado debido a un nombre de tabla desconocido de SQL.
RC_FS_NOTCAP	ERROR	29	El mandato ha fallado debido a los tipos de nombres de espacio de archivo no compatibles.
RC_INVALIDADDR	ERROR	30	El mandato ha fallado porque hay una dirección de alto nivel o una dirección de bajo nivel incorrectas.
RC_INVALIDCG	ERROR	31	El mandato ha fallado porque la clase de gestión no tiene un grupo de copia de archivado.
RC_OVERSIZE_VOL	ERROR	32	El mandato ha fallado porque el tamaño del volumen supera el máximo permitido.

Código de retorno	Gravedad	Valor numérico	Descripción
RC_DEFVOL_FAIL	ERROR	33	El mandato ha fallado porque los volúmenes no se pueden definir en las agrupaciones de almacenamiento de RECLAMATIONTYPE=SNAPLOCK.
RC_DELVOL_FAIL	ERROR	34	El mandato ha fallado porque los volúmenes no se pueden suprimir en las agrupaciones de almacenamiento de RECLAMATIONTYPE=SNAPLOCK.
RC_CANCELED	AVISO	35	El mandato se ha cancelado.
RC_INVPOLICY	ERROR	36	El mandato ha fallado porque hay una definición no válida en el dominio de políticas.
RC_INVALIDPW	ERROR	37	El mandato ha fallado porque hay una contraseña no válida.
RC_UNSUPP_PARM	AVISO	38	El mandato ha fallado porque el mandato o el parámetro no es compatible.

Referencia relacionada:

DEFINE SCRIPT (definir un script de IBM Spectrum Protect)

UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)

RUN (ejecutar un script de IBM Spectrum Protect)

Documentación de servidor en archivos PDF

Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

Consejo: A partir de la V7.1.3, la *Guía de usuario del administrador* queda obsoleta. Utilice las guías de la solución para implementar y gestionar una solución de disco de un solo sitio y una solución de disco de varios sitios. Los procedimientos para realizar las tareas de administración del sistema están disponibles en los siguientes temas:

- Configuración y gestión del entorno de almacenamiento
- Soluciones de protección de datos IBM Spectrum Protect

Para completar las tareas siguientes, consulte los archivos PDF en los enlaces siguientes.

Tarea	Componentes	Enlaces
Información sobre conceptos de producto y soluciones	<ul style="list-style-type: none"> • Servidor • Centro de operaciones 	Introducción a las soluciones de protección de datos
Despliegue de una solución de mejores prácticas	<ul style="list-style-type: none"> • Servidor • Centro de operaciones 	<ul style="list-style-type: none"> • Guía de solución de disco con un solo sitio • Guía de solución de disco con varios sitios • Guía de soluciones de cintas
Instalación de componentes	<ul style="list-style-type: none"> • Servidor • Centro de operaciones 	<ul style="list-style-type: none"> • AIX • Linux • Windows
Actualización de componentes	<ul style="list-style-type: none"> • Servidor 	<ul style="list-style-type: none"> • AIX • Linux • Windows
Uso de mandatos y opciones	<ul style="list-style-type: none"> • Servidor 	<ul style="list-style-type: none"> • AIX • Linux • Windows
Uso de mensajes y códigos de error	<ul style="list-style-type: none"> • Servidor 	Todos los sistemas operativos

Cientes de archivado y copia de seguridad de IBM Spectrum Protect

Utilice el cliente de archivado y copia de seguridad de IBM Spectrum Protect para guardar las copias de archivos y directorios de su estación de trabajo o servidor de archivos y almacenarlos en el servidor de IBM Spectrum Protect. En caso de que los archivos originales queden dañados o se pierdan, podrá recuperar estas copias. Dependiendo de sus motivos para guardar los datos, puede hacer una copia de seguridad o archivar los datos.

Este release no incluye una versión actualizada del componente de cliente de copia de seguridad y archivado. Para obtener la documentación de cliente de archivado y copia de seguridad, consulte los releases anteriores.

Interfaz de programación de aplicaciones

La interfaz de programación de aplicaciones (API) de IBM Spectrum Protect está empaquetada con el cliente de copia de seguridad y archivado de IBM Spectrum Protect. Con la API, puede proteger aplicaciones de negocio, como aplicaciones de bases de datos, en el entorno de IBM Spectrum Protect.

Este release no incluye una versión actualizada del componente de API. Para obtener la documentación de API, consulte los releases anteriores.

Rendimiento

Existen muchos factores que afectan el rendimiento del servidor y de los clientes, incluyendo sistemas operativos, sistema de hardware, configuraciones de red, tipos de dispositivos de almacenamiento y tamaños y números de archivos de cliente. Las interacciones entre estos factores pueden hacer que la optimización del rendimiento sea compleja.

En este release no se incluye una versión actualizada del componente de rendimiento. Para obtener la documentación que trata sobre el rendimiento, consulte la Versión 8.1.0.

Resolución de problemas

Hay procedimientos de resolución de problemas disponibles para el diagnóstico y la resolución de problemas.

Este release no incluye una versión actualizada del componente de resolución de problemas. Para obtener la documentación que trata sobre la resolución de problemas, consulte la Versión 8.1.0.

Mensajes, códigos de retorno y códigos de error

Hay disponibles explicaciones y acciones recomendadas para los mensajes emitidos por los componentes de IBM Spectrum Protect.

- Introducción a los mensajes
- Mensajes ANS 0000-9999
- Códigos de retorno de API
- Códigos de retorno de IBM Global Security Kit
El servidor y el cliente utilizan el proceso de IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre el servidor y el cliente de archivado y copia de seguridad. Algunos mensajes que se emiten para el proceso de SSL incluyen códigos de retorno de GSKit.
- ANE: eventos del cliente registrados en el servidor
- ANR: mensajes comunes del servidor y específicos de la plataforma
- Descripciones de código de error de E/S en mensajes de servidor
- Códigos de error de dispositivo en el registro de errores del sistema AIX
- [Resolución de problemas \(V8.1.0 es la publicación más reciente\)](#)

Introducción a los mensajes

Los mensajes, códigos de error y códigos de retorno son emitidos por el servidor y los clientes de IBM Spectrum Protect.

Los mensajes y los códigos pueden aparecer en la consola del servidor, el cliente administrativo, una terminal del operador, la interfaz gráfica de usuario administrativa, el cliente de archivado y copia de seguridad o el cliente de gestión de almacenamiento jerárquico (cliente HSM).

IBM Spectrum Protect proporciona anotaciones de actividades para ayudar al administrador a hacer un seguimiento de la actividad del servidor y a supervisar el sistema. Las anotaciones de actividad contienen los mensajes que genera el servidor, y están almacenadas en la base de datos. El servidor elimina automáticamente los mensajes de las anotaciones de actividad una vez expirado el período de

retención. Los mensajes de error enviados a la consola del servidor se almacenan en las anotaciones de actividades. Ejemplos de tipos de mensajes almacenados en las anotaciones de actividades incluyen:

- Cuándo se inician o finalizan las sesiones de cliente.
- Cuándo se inicia o finaliza la migración.
- Cuándo han caducado los archivos de copia de seguridad del almacenamiento del servidor
- Cualquier salida generada desde los procesos de fondo

Algunos mensajes no tienen explicaciones y no se publican. El cliente puede enviar estadísticas al servidor que proporciona la información sobre una copia de seguridad o restauración. Esas estadísticas son mensajes informativos que pueden activarse o desactivarse en los varios receptores de anotaciones de eventos. Estos mensajes no se publican.

- Formato de los mensajes de cliente y servidor de IBM Spectrum Protect
- Interpretación de los mensajes de código de retorno

Tareas relacionadas:

🔗 [Uso del registro de actividad \(V7.1.1\)](#)

Formato de los mensajes de cliente y servidor de IBM Spectrum Protect

Los mensajes de cliente y servidor IBM Spectrum Protect constan de los siguientes elementos:

- Un prefijo de tres letras. Los mensajes tiene distintos prefijos que ayudan a identificar el componente IBM Spectrum Protect que emite el mensaje. Generalmente, todos los mensajes de un componente tienen el mismo prefijo. A veces un componente emite mensajes con dos o tres prefijos diferentes.

Por ejemplo, los clientes de archivado y copia de seguridad emiten mensajes con el prefijo ANS. Los eventos de cliente de archivado y copia de seguridad que se registran en el servidor tienen el prefijo ANE. Los mensajes comunes del servidor y específicos de la plataforma del servidor tienen el prefijo ANR.

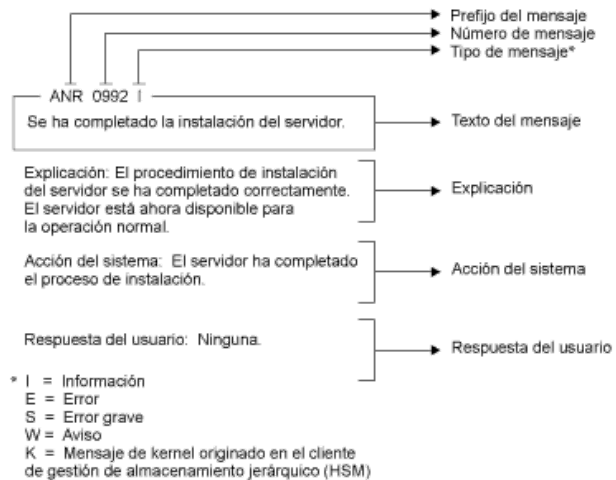
- Identificador de mensaje numérico.
- Un código de gravedad de una letra. Los códigos siguientes indican la gravedad de la acción que ha generado el mensaje:

Código	Gravedad	Significado
S	Grave	El producto o una función del producto no puede continuar. Es necesaria una respuesta del usuario.
E	Error	Se ha encontrado un error durante el proceso. El proceso puede llegar a detenerse. Puede ser necesaria una respuesta del usuario.
Sem	Aviso	El proceso continúa, pero pueden producirse problemas más adelante como resultado del aviso.
I	Información	El proceso continúa. No es necesaria ninguna respuesta por parte del usuario.

- Un mensaje de texto que se muestra en pantalla y está escrito en las anotaciones de mensajes.
- Textos Explicación, Acción del sistema, y Respuesta del usuario. Estos textos se profundizan en el texto de mensaje y están disponibles en las publicaciones de mensajes de producto y en la ayuda de línea de mandatos.

La imagen siguiente presenta un mensaje de servidor de IBM Spectrum Protect típico.

Los globos identifican cada elemento del mensaje.



Las variables de mensaje del texto del mensaje aparecen en cursiva.

Interpretación de los mensajes de código de retorno

Muchos mandatos distintos pueden generar el mismo *código de retorno*. Los siguientes ejemplos son ilustraciones de dos mandatos distintos emitidos que producen el mismo código de retorno; por lo tanto, debe leer el *mensaje descriptivo* para el mandato.

En estos ejemplos, dos mandatos diferentes proporcionan el mismo código de retorno, pero también devuelven mensajes descriptivos que son únicos para cada mandato. Los dos mandatos son `q event standard dddd y def vol cstg05 primary`. Ambos proporcionan un mensaje genérico con un código de retorno:

ANS5102I: Código de retorno 11.

Pero el primer mandato también proporciona un mensaje descriptivo:

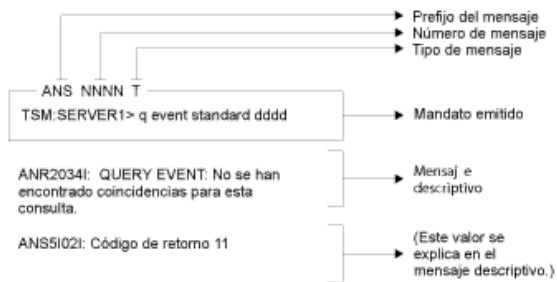
ANR2034I: QUERY EVENT: No se ha encontrado coincidencia para esta consulta.

Y el segundo mandato también proporciona un mensaje único descriptivo:

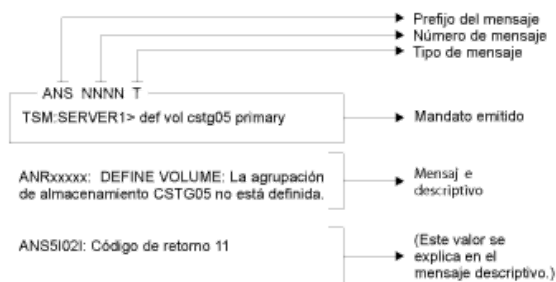
ANRxxxx: DEFINE VOLUME: No se ha definido la agrupación de almacenamiento CSTG05.

- Ejemplo uno para el mandato QUERY EVENT
- Ejemplo dos para el mandato DEFINE VOLUME

Ejemplo uno para el mandato QUERY EVENT



Ejemplo dos para el mandato DEFINE VOLUME



Mensajes de ANE

El servidor emite los mensajes de ANE. Todos los mensajes con prefijo ANE son sucesos de cliente registrados en el servidor.

- Lista de mensajes de ANE

Mensajes de ANR

El servidor emite los mensajes de ANR. Algunos mensajes ANR son comunes para todos los sistemas operativos, y algunos son específicos a un único sistema operativo.

- Lista de mensajes de ANR

Mensajes ANS 0000-9999

Este release no incluye los mensajes actualizados con el prefijo ANS. Para obtener la documentación de los mensajes con el prefijo ANS, consulte otros releases de IBM Spectrum Protect.

Códigos de retorno de API

Este release no incluye los códigos de retorno actualizados de la interfaz de programación de aplicaciones (API). Para obtener información sobre códigos de retorno de API, consulte otros releases de IBM Spectrum Protect.

Descripciones de los códigos de E/S en mensajes del servidor

Los mensajes de IBM Spectrum Protect pueden contener códigos de entrada/salida (E/S). Los códigos pueden ser códigos de operación, códigos de terminación, códigos de detección adicionales (ASC) y códigos de cualificador de código de detección adicionales (ASCQ).

El servidor de IBM Spectrum Protect proporciona descripciones de códigos para los mensajes de error de E/S para todos los sistemas operativos compatibles.

Código

Descripción

OP

La operación de E/S que falló. Estos valores se pueden visualizar:

- LECTURA
- GRABACIÓN
- FSR (registro de espaciado hacia delante)
- RSR (registro de espacio inverso)
- FSF (archivo de espaciado hacia delante)
- RSF (archivo de espacio inverso)
- WEOF (escribir marca final de archivo)
- OFFL (retroceder y descargar la cinta)
- FLUSH (vaciado)
- GET_MEDIUM_INFO (obtener información del medio)
- LOCATE (localización)
- QRYLBP (protección de bloqueo lógico de consulta)
- RDBLKID (ID de bloque de lectura)
- SETLBP (establecer protección de bloqueo lógico)
- SETMODE (establecer modo)
- REW (retroceder)
- SPACEEOD (espacio de fin de datos)
- TESTREADY (unidad de prueba lista)

CC

Código de terminación de E/S. El controlador de dispositivo devuelve este valor al servidor cuando se produce un error. Para obtener una lista de códigos de terminación, consulte Visión general de los valores de los códigos de terminación y de operación. Para obtener información acerca de las llamadas al sistema de la biblioteca de cintas y las descripciones de errores de las solicitudes de control de E/S de la biblioteca, consulte la Nota técnica S7002972.

CLAVE

Byte 2 de los bytes de detección a partir del error. Las listas siguientes muestran algunas definiciones:

- 0 = no hay bytes de detección adicionales disponibles
- 1 = error recuperado
- 2 = no preparado
- 3 = error medio
- 4 = error de hardware
- 5 = solicitud incorrecta
- 6 = unit attention (por ejemplo, un restablecimiento de bus SCSI)
- 7 = proteger datos
- 8 = selección en blanco
- 9 = proveedor específico
- A = copia cancelada
- B = mandato cancelado
- C = obsoleto
- D = desbordamiento de volumen
- E = comparación errónea
- F = reservado

ASC/ASCQ

Los códigos ASC y ASCQ son los bytes 12 y 13 de los bytes de detección. El manual de referencia de la unidad o biblioteca proporcionado con el dispositivo contiene tablas que explican los valores de los campos KEY, ASC y ASCQ. Descripciones de códigos estándar ASC y ASCQ proporciona información adicional acerca de valores estándares de códigos ASC y ASCQ.

Códigos de error de sistema operativo

Cuando un mandato falla, el sistema operativo devuelve un número de error. Para determinar qué significan los códigos de error, realice la siguiente acción:

- En las plataformas AIX, HP-UX y Solaris, vea el archivo `errno.h` en el directorio `/usr/include/sys`. Este archivo proporciona definiciones para códigos de error.
- En plataformas Linux, vea los archivos `errno-base.h` y `errno.h` en el directorio `/usr/include/asm-generic`. Estos archivos proporcionan definiciones para códigos.
- En las plataformas de Windows, contacte con el soporte de Microsoft para obtener ayuda con los mensajes de error.
- Visión general de los valores de los códigos de terminación y de operación
Los mensajes de IBM Spectrum Protect pueden contener códigos de terminación de controlador de dispositivo de los controladores de dispositivos.
- Descripciones de códigos estándar ASC y ASCQ
Se describen códigos ASC y ASCQ estándares.

Visión general de los valores de los códigos de terminación y de operación

Los mensajes de IBM Spectrum Protect pueden contener códigos de terminación de controlador de dispositivo de los controladores de dispositivos.

- Códigos de terminación de controladores de dispositivos: códigos comunes
IBM Spectrum Protect los controladores de dispositivos proporcionan códigos de terminación que son comunes a todas las clases de dispositivos.
- Códigos de terminación de controladores de dispositivos: cambiadores de medios
IBM Spectrum Protect controladores de dispositivos proporcionan códigos de terminación que son específicos para dispositivos cambiadores de medios.
- Códigos finalización de controladores del dispositivo: unidades de cinta
IBM Spectrum Protect los controladores de dispositivo proporcionan códigos de finalización que son específicos de las unidades de cinta.

Códigos de terminación de controladores de dispositivos: códigos comunes

IBM Spectrum Protect los controladores de dispositivos proporcionan códigos de terminación que son comunes a todas las clases de dispositivos.

La siguiente tabla muestra valores de códigos de terminación para los controladores de dispositivos IBM Spectrum Protect. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de completar la acción recomendada, vuelva a intentar la operación que falló.

Tabla 1. Valores del código de terminación comunes a todas las clases de dispositivos

Decimal	Hexadecimal	Descripción	Acción recomendada
200	X'C8'	El dispositivo ha indicado una condición de error, pero no hay disponibles datos de detección.	Vuelva a intentar la operación que falló.
201	X'C9'	El controlador del dispositivo ha fallado.	Contacte con el soporte de IBM Spectrum Protect.
202	X'CA'	El dispositivo EEPROM ha fallado.	Compruebe el dispositivo. Sirva el dispositivo si es necesario.
203	X'CB'	Se necesita intervención manual.	Corrija el problema en el dispositivo. El problema puede ser una cinta atascada, cabezales sucios o una sección de la biblioteca atestada.
204	X'CC'	El sistema se ha recuperado de un error de E/S; solo para su información.	No es necesaria ninguna acción.

Decimal	Hexadecimal	Descripción	Acción recomendada
205	X'CD'	El adaptador SCSI ha fallado.	Compruebe los cables sueltos, patillas dobladas, cables dañados, adaptadores SCSI malos, terminaciones incorrectas o terminadores malos.
206	X'CE'	Se ha producido un error SCSI general.	Compruebe los cables sueltos, patillas dobladas, cables dañados, adaptadores SCSI malos, terminaciones incorrectas o terminadores malos.
207	X'CF'	El dispositivo no puede llevar a cabo la acción solicitada.	Asegúrese de que el dispositivo está encendido y preparado. Asegúrese de que la unidad se ha definido correctamente con el mandato DEFINE DRIVE. Asegúrese de que la clase de dispositivo se definió correctamente con el mandato DEFINE DEVCLASS.
208	X'D0'	El mandato finaliza.	Contacte con el soporte de IBM Spectrum Protect.
209	X'D1'	Se ha detectado un error en el microcódigo del dispositivo.	Compruebe el nivel de microcódigo de la unidad. Contacte con el fabricante de la unidad y solicite el nivel más reciente.
210	X'D2'	El dispositivo se ha restablecido debido a encendido de dispositivo, restablecimiento de bus SCSI o carga/expulsión manual de cinta.	Vuelva a intentar la operación que falló.
211	X'D3'	El bus de SCSI está ocupado.	Asegúrese de que los ID de SCSI están correctamente asignados al dispositivo correcto, y que ningún otro proceso está accediendo al dispositivo.
212	X'D4'	La reserva persistente no es compatible en este dispositivo.	No es necesario realizar ninguna acción.
213	X'D5'	Ha fallado una operación de reserva persistente.	Restablezca el dispositivo e intente la operación de nuevo. Si el problema persiste, póngase en contacto con Soporte IBM Spectrum Protect.

Códigos de terminación de controladores de dispositivos: cambiadores de medios

IBM Spectrum Protect controladores de dispositivos proporcionan códigos de terminación que son específicos para dispositivos cambiadores de medios.

La siguiente tabla muestra valores de códigos para los controladores de dispositivos IBM Spectrum Protect para cambiadores de medios. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de realizar la acción recomendada, vuelva a intentar la operación que falló.

Tabla 1. Valores del código de terminación para cambiadores de medios

Decimal	Hexadecimal	Descripción	Acción recomendada
300	X'12C'	Error de entrada/salida de cartucho	Compruebe los puertos de entrada/salida o la biblioteca.
301	X'12D'	Error de carga de cartucho	Compruebe la unidad para volúmenes atascados. En AIX, despliegue el errpt para comprobar los errores de hardware.
302	X'12E'	Cartucho en unidad con errores	Compruebe la unidad para volúmenes atascados. En AIX, despliegue el errpt para comprobar los errores de hardware.

Decimal	Hexadecimal	Descripción	Acción recomendada
303	X'12F'	Carrusel no cargado	Asegúrese de que el carrusel está correctamente en su lugar y la puerta cerrada.
304	X'130'	Error de cambiador	En AIX, despliegue el errpt para comprobar los errores de hardware.
305	X'131'	Error de unidad	Asegúrese de que los cabezales están limpios. En AIX, despliegue el errpt para comprobar los errores de hardware.
306	X'132'	Error de unidad o de medios	Asegúrese de que los cabezales están limpios. En AIX, despliegue el errpt para comprobar los errores de hardware.
307	X'133'	Error de entrada/salida	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
308	X'134'	Puerto de entrada/salida ausente	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
309	X'135'	Error de auditoría de biblioteca	Asegúrese de que no hay volúmenes atascados. Es posible que la auditoría de la biblioteca esté fallando debido a los errores de hardware. En AIX, despliegue el errpt para comprobar los errores de hardware.
310	X'136'	Biblioteca llena	Compruebe los volúmenes atascados. Asegúrese de que los volúmenes no se han reorganizado. Si la biblioteca no está llena, inicie el mandato AUDIT LIBRARY.
311	X'137'	Exportación de medios	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
312	X'138'	Error de ranura	Asegúrese de que no hay nada atascado en la ranura.
313	X'139'	Error de ranura o de medios	Asegúrese de que el volumen no está atascado en la ranura y de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
314	X'13A'	La ranura o unidad origen estaba vacía al intentar trasladar un volumen	Asegúrese de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
315	X'13B'	La ranura o unidad destino estaba llena al intentar trasladar un volumen	Asegúrese de que los volúmenes no se han reorganizado, o de que no hay ningún volumen atascado en la unidad. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
316	X'13C'	Cartucho limpiador instalado	Póngase en contacto con el soporte de IBM Spectrum Protect .
317	X'13D'	El medio no se ha rechazado	Asegúrese de que los volúmenes no se han reorganizado, o de que no hay ningún volumen atascado en la unidad. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
318	X'13E'	Puerto E/S no configurado	Contacte con el soporte de IBM Spectrum Protect.

Decimal	Hexadecimal	Descripción	Acción recomendada
319	X'13F'	Primer destino vacío	Asegúrese de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
320	X'140'	No hay información del inventario	Inicie el mandato AUDIT LIBRARY.
321	X'141'	Lea la no coincidencia del estado del elemento	Asegúrese de que el firmware y los controladores de adaptador de bus de host están en los niveles actuales. Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
322	X'142'	Inicialice el rango que ha fallado	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.

Códigos finalización de controladores del dispositivo: unidades de cinta

IBM Spectrum Protect los controladores de dispositivo proporcionan códigos de finalización que son específicos de las unidades de cinta.

La tabla siguiente muestra los valores de códigos de finalización para los IBM Spectrum Protect controladores del dispositivo para unidades de cinta. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de intentar una acción recomendada, intente la operación fallida de nuevo.

Tabla 1. Valores de código de finalización para controladores de cinta

Decimal	Hexadecimal	Descripción	Acción recomendada
400	X'190'	Detectado final físico de medio	Asegúrese de que los cabezales de la unidad están limpios.
401	X'191'	Detectado el fin de los datos	Contacte con el soporte de IBM Spectrum Protect.
402	X'192'	Medio dañado	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
403	X'193'	Error de medios	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
404	X'194'	Incompatibilidad de medios	Asegúrese de que se está utilizando la longitud y el tipo de medio correcto.
406	X'196'	El sector solicitado no es válido	Error interno del servidor. Contacte con el soporte de IBM Spectrum Protect.
407	X'197'	Protegido contra grabación	Asegúrese de que el volumen no está protegido contra escritura.
408	X'198'	Limpiar el medio y la unidad	Limpie los cabezales de unidad con un cartucho de limpieza.
409	X'199'	Anomalía en el medio	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
410	X'19A'	Limpieza completada	Vuelva a intentar la operación que falló.
411	X'19B'	Detectado final lógico de medio	Contacte con el soporte IBM Spectrum Protect.

Decimal	Hexadecimal	Descripción	Acción recomendada
412	X'19C'	El medio no se encuentra en la unidad	Asegúrese de que la unidad esté correctamente colocado en el archivo. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
413	X'19D'	Se ha encontrado el inicio del medio	Contacte con el soporte de IBM Spectrum Protect.
414	X'19E'	Anomalía en la operación de borrado	Limpiar los cabezales de la unidad.
415	X'19F'	Se ha intentado sobregabar un medio WORM grabado	Error interno del servidor. Contacte con el soporte IBM Spectrum Protect.
416	X'1A0'	Se ha leído un bloque de longitud incorrecta	Asegúrese de que los cabezales están limpios. En AIX, despliegue el errpt para comprobar los errores de hardware.
417	X'1A1'	Abrir sólo lectura	Contacte con el soporte de IBM Spectrum Protect.
418	X'1A2'	Abrir sólo escritura	Contacte con el soporte de IBM Spectrum Protect.
419	X'1A2'	Ha fallado la exploración de medio	Limpiar el medio y la unidad
420	X'1A4'	Protegido contra grabación lógica	Asegúrese de que los cabezales están limpios. Compruebe las anotaciones de errores del sistema operativo para los errores de hardware. Verifique que se ha quitado la pestaña de protección contra grabación. Apague la aceleración de cinta SAN o establezca CHECKTAPEPOS en OFF o TSMonly.
422	X'1A6'	Es necesaria la limpieza	Limpiar la unidad de cinta.
423	X'1A7'	Error de medios	Compruebe las anotaciones de errores del sistema operativo para los errores de hardware. Compruebe los medios dañados.
424	X'1A8'	Se ha producido un error relacionado con el cifrado	Compruebe el ajuste de cifrado de la clase de dispositivo y de la unidad de cinta.
425	X'1A9'	Se ha producido un error relacionado con el descifrado	Compruebe el ajuste de cifrado de la clase de dispositivo y de la unidad de cinta.
425	X'1AA'	Se ha producido un error externo relacionado con el cifrado	Compruebe el valor de cifrado en la clase de dispositivo y la unidad de cintas.
426	X'1AB'	Se ha producido un error de coincidencia de CRC	Asegúrese de que el medio no ha alcanzado el final de vida especificado por el fabricante de medios. Vuelva a intentar la operación.

Descripciones de códigos estándar ASC y ASCQ

Se describen códigos ASC y ASCQ estándares.

Los códigos ASC y ASCQ son dispositivos de 12 y 13 bytes para SCSI-2. En sistemas de Windows estos códigos se muestran en el registro de sucesos de Windows, pero la información se encuentra en bytes distintos.

Consulte el mensaje del servidor ANR8300E o ANR8302E para la acción recomendada.

La tabla siguiente ofrece descripciones estándar para algunos códigos ASC y ASCQ. Cada uno de los valores tiene un prefijo de 0x, que indica que es una constante hexadecimal. Observe que las descripciones varían según el dispositivo. Para obtener una descripción precisa de códigos ASC y ASCQ para cualquier dispositivo, consulte la documentación que acompaña al dispositivo.

Tabla 1. Descripciones de códigos estándar ASC y ASCQ

ASC	ASCQ	Descripción
-----	------	-------------

ASC	ASCQ	Descripción
0x00	0x00	No hay detección adicional
0x00	0x01	Detectada marca de archivo
0x00	0x02	Detectado fin de medio
0x00	0x03	Detectada marca de conjunto
0x00	0x04	Comienzo de medio
0x00	0x05	Fin de los datos
0x00	0x06	Proceso E/S terminado
0x02	0x00	No hay búsqueda completada
0x03	0x00	Anomalía de grabación del dispositivo
0x03	0x01	No hay grabación actual
0x03	0x02	Demasiados errores de grabación
0x04	0x00	Unidad lógica no preparada
0x04	0x01	Comienzo preparado
0x04	0x02	No preparado, se necesita inicialización del mandato
0x04	0x03	No preparado, se necesita la intervención manual
0x04	0x04	No preparado, formateando
0x05	0x00	No hay respuesta a seleccionar
0x06	0x00	No se ha encontrado posición de referencia
0x07	0x00	Seleccionados múltiples dispositivos
0x08	0x00	Anomalía en la comunicación
0x08	0x01	Tiempo de espera de la comunicación
0x08	0x02	Error de paridad de comunicación
0x09	0x00	Realizar seguimiento del siguiente error
0x0A	0x00	Desbordamiento de las anotaciones de errores.
0x0C	0x00	Error de grabación
0x11	0x00	Error de lectura no recuperado
0x11	0x01	Se han agotado los reintentos de lectura
0x11	0x02	Error demasiado largo para corregirlo
0x11	0x03	Múltiples errores de lectura
0x11	0x08	Lectura de bloque incompleta
0x11	0x09	No se han encontrado huecos
0x11	0x0A	Error mal corregido
0x14	0x00	Entidad grabada no encontrada
0x14	0x01	Registro no encontrado
0x14	0x02	Marca de archivo/marca de conjunto no encontrado
0x14	0x03	Fin de los datos no encontrado
0x14	0x04	Error de secuencia de bloques
0x15	0x00	Error de posicionamiento aleatorio
0x15	0x01	Error de posicionamiento mecánico
0x15	0x02	Error de posicionamiento de lectura
0x17	0x00	No se ha aplicado error de corrección
0x17	0x01	Recuperado con reentradas

ASC	ASCQ	Descripción
0x17	0x02	Recuperado con desplazamiento positivo de cabezales
0x17	0x03	Recuperado con desplazamiento negativo de cabezales
0x18	0x00	ECC aplicado
0x1A	0x00	Error de longitud de la lista de parámetros
0x1B	0x00	Error de transferencia síncrona de datos
0x20	0x00	Código de operación no válido
0x21	0x00	Bloque fuera del rango permitido
0x21	0x01	Dirección de elemento no válida
0x24	0x00	Campo no válido en CDB
0x25	0x00	LUN no admitido
0x26	00	Campo no válido en la lista de parámetros
0x26	0x01	Parámetro no admitido
0x26	0x02	Valor de parámetro no admitido
0x26	0x03	Parámetros de umbral no admitidos
0x27	0x00	Protegido contra la grabación
0x28	0x00	No preparado a preparado
0x28	0x01	Se accedió al elemento importar/exportar
0x29	0x00	Conexión, restablecimiento, restablecimiento de bus
0x2A	0x00	Parámetros cambiados
0x2A	0x01	Parámetros de modalidad cambiados
0x2A	0x02	Parámetros de anotación cambiados
0x2B	0x00	No se puede ejecutar la copia
0x2C	0x00	Error de secuencia de mandato
0x2D	0x00	Sobrescribir error en la actualización
0x2F	0x00	mandato limpiado por el iniciador
0x30	0x00	Medio incompatible
0x30	0x01	Formato de medio desconocido
0x30	0x02	Formato de medio incompatible
0x30	0x03	Cartucho limpiador instalado
0x31	0x00	Formato de medio corrupto
0x33	0x00	Error de longitud de la cinta
0x37	0x00	Parámetro redondeado
0x39	0x00	Guardando parámetros no admitidos
0x3A	0x00	Medio no presente
0x3B	0x00	Error de posicionamiento secuencial
0x3B	0x01	Error de posicionamiento en BOT
0x3B	0x02	Error de posicionamiento en EOT
0x3B	0x08	Error de recolocación
0x3B	0x0D	Elemento de destino de medio lleno
0x3B	0x0E	Elemento de origen de medio vacío
0x3D	0x00	Bits no válidos en el mensaje
0x3E	0x00	LUN no auto-configurado

ASC	ASCQ	Descripción
0x3F	0x00	Condiciones operativas cambiadas
0x3F	0x01	Ha cambiado el microcódigo
0x3F	0x02	Definición operativa cambiada
0x3F	0x03	Han cambiado los datos de consulta
0x3F	0x0E	Han cambiado los datos LUN indicados
0x43	0x00	Mensaje de error
0x44	0x00	Anomalía interna de destino
0x45	0x00	Anomalía seleccionar/volver a seleccionar
0x46	0x00	Restablecimiento de software sin éxito
0x47	0x00	Error de paridad SCSI
0x48	0x00	Iniciador detectado mensaje recibido
0x49	0x00	Error de mensaje no válido
0x4A	0x00	Error de fase de mandato
0x4B	0x00	Error de fase de datos
0x4C	0x00	LUN ha fallado la auto-configuración
0x4E	0x00	Intento de mandatos solapados
0x50	0x00	Error para añadir grabación
0x50	0x01	Error de posición para añadir grabación
0x50	0x02	Error de posición (temporización)
0x51	0x00	Anomalía en la operación de borrado
0x52	0x00	Anomalía del cartucho
0x53	0x00	Ha fallado la expulsión de carga/medio
0x53	0x01	Anomalía de cinta no cargada
0x53	0x02	Eliminación de medios impedida
0x5A	0x00	Estado de la operación cambiado
0x5A	0x01	Eliminación de los medios del operador
0x5A	0x02	Protegido contra grabación del operador
0x5A	0x03	Permitida la grabación del operador
0x5B	0x00	Excepción de anotaciones
0x5B	0x01	Se cumplió la condición de umbral
0x5B	0x02	Contador de anotaciones al máximo
0x5B	0x03	Se han agotado los códigos de lista de anotaciones

- Códigos ASC y ASCQ en el registro de sucesos de Windows
Los códigos ASC y ASCQ se visualizan en el registro de sucesos de Windows.

Códigos de error de dispositivo en el registro de errores del sistema AIX

Algunos códigos de error de dispositivo se registran en el registro de errores del sistema AIX.

ADSM_DD_LOG1 (0xAC3AB953)
DEVICE DRIVER SOFTWARE ERROR

Este error se ha registrado por el controlador de dispositivo IBM Spectrum Protect cuando se sospecha que hay un problema en el software del controlador de dispositivo IBM Spectrum Protect. Si el controlador de dispositivo IBM Spectrum Protect emite un mandato de E/S SCSI con un código de operación ilegal, el mandato falla y el error se registra con este identificador. Informe de este error inmediatamente al personal de soporte de IBM Spectrum Protect.

Datos de detalle: Datos de detección

Los datos de detección contienen información que puede determinar la causa del error. Informe de todos los datos de la entrada de error al personal de soporte de IBM Spectrum Protect.

ADSM_DD_LOG2 (0x5680E405)
HARDWARE/COMMAND-ABORTED ERROR

Este error lo registra el controlador del dispositivo de IBM Spectrum Protect si el dispositivo emite un error de hardware o un error de mandato cancelado en respuesta a un mandato E/S SCSI.

Datos de detalle: Datos de detección

Los datos de detección contienen información que pueden determinar qué componente de hardware ha fallado y por qué. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM_DD_LOG3 (0x461B41DE)
MEDIA ERROR

El controlador de dispositivo IBM Spectrum Protect registra este error cuando falla el mandato de I/O de SCSI, o porque el disco requiere una limpieza.

Datos de detalle: Datos de detección

Los datos de detección contienen información que puede determinar la causa del error. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM_DD_LOG4 (0x4225DB66)
TARGET DEVICE GOT UNIT ATTENTION

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir determinadas notificaciones UNIT ATTENTION desde el dispositivo. Las UNIT ATTENTION son informativas y, normalmente, indican que algún estado del dispositivo ha cambiado. Por ejemplo, se registraría este error si la puerta de un dispositivo de biblioteca se abriera y después se cerrara. El registro de este suceso indica que la actividad se produjo y que es posible que el inventario de la biblioteca haya cambiado.

Datos de detalle: Datos de detección

Los datos de detección contienen información que describen la causa para emitir una notificación UNIT ATTENTION. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM_DD_LOG5 (0xDAC55CE5)
PERMANENT UNKNOWN ERROR

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir un error desconocido desde un dispositivo en respuesta al mandato de I/O de SCSI. Si el problema persiste, póngase en contacto con el personal de soporte de IBM Spectrum Protect.

Datos de detalle: Datos de detección

Los datos de detección constan de información que puede determinar la causa del error. Informe de todos los datos de la entrada de error al personal de soporte de IBM Spectrum Protect.

ADSM_DD_LOG6 (0xBC539B26)
WARNING OR INFORMATIONAL MESSAGE FOR TARGET DEVICE

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir una advertencia o un mensaje informativo desde un dispositivo en respuesta a un mandato de I/O de SCSI. Son mensajes informativos y pueden no ser indicativos de un problema. Si el problema persiste, notifíquese al soporte de IBM Spectrum Protect.

Datos de detalle: Datos de detección

Los datos de detección constan de información que puede determinar la causa del mensaje. Informe de todos los datos de la entrada al personal de soporte de IBM Spectrum Protect.

Códigos de retorno de IBM Global Security Kit

El servidor y el cliente utilizan el proceso de IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre el servidor y el cliente de archivado y copia de seguridad. Algunos mensajes que se emiten para el proceso de SSL incluyen códigos de retorno de

GSKit.

GSKit se instala o actualiza automáticamente durante la instalación de IBM Spectrum Protect y proporciona las bibliotecas siguientes:

- SSL de GSKit
- API de gestión de claves GSKit
- IBM Crypto for C (ICC)

Los informes del programa de utilidad tsmdiag notifican el nivel de GSKit que se ha instalado en el sistema o puede utilizar uno de estos métodos:

- Para Windows, emita los mandatos siguientes:

```
regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"
notepad gskitinfo.txt
```

PRECAUCIÓN:

Puede dañar el registro del sistema si utiliza regedit de forma incorrecta.

- Para el servidor AIX de 64 bits, emita el siguiente mandato desde la línea de mandatos: `gsk8ver_64`

Consulte la Tabla 1 para ver los códigos de retorno SSL de GSKit.

El servidor utiliza la API de gestión de claves GSKit para crear automáticamente la base de datos de gestión de claves y las claves públicas y privadas del servidor. Algunos mensajes que se emiten para este proceso pueden incluir códigos de retorno de gestión de claves GSKit. Consulte la Tabla 2 para ver los códigos de retorno de gestión de claves.

Tabla 1. Códigos de retorno generales de IBM Global Security Kit SSL

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Lo emite cada llamada de función que se completa correctamente.
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función <code>open()</code> correcta.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.
0x00000005	5	GSK_INVALID_STATE	El manejador tiene un estado no válido para la operación como, por ejemplo, realizar una operación <code>init()</code> en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar la criptografía.
0x0000000a	10	GSK_ERROR_ASN	Error al validar los campos ASN del certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x0000000d	13	GSK_INVALID_PARAMETER	Parámetro no válido.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Parámetro no válido. Informe de este error al servicio de soporte de software de IBM.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves no tiene un formato interno válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlace dinámico GSK. Asegúrese de que GSK se ha instalado correctamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido GSK_ENVIRONMENT_CLOSE_OPTIONS en GSK_DELAYED_ENVIRONMENT_CLOSE y se ha llamado a la función <code>gsk_environment_close()</code> .
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el nombre del archivo stash. El archivo de claves no se ha inicializado.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Una contraseña utilizada para una consulta LDAP (lightweight directory access protocol) no es correcta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato <code>gsk_secure_socket*()</code> después de una llamada a <code>gsk_close_environment()</code> .
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema no se ha establecido en un valor válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña especificada para el archivo de claves no es correcta. No se puede utilizar el archivo de claves. Es posible también que el archivo de claves esté dañado.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.
0x0000019b	411	GSK_ERROR_BAD_MAC	El código de autenticación de mensaje (MAC) no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	No se ha recibido un protocolo SSL válido del socio.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	<code>read()</code> ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	<code>write()</code> ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El cifrado de la versión especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El cifrado de la versión 3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	No se puede crear el manejador. Informe de este error al servicio de soporte de software de IBM.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	La inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	El controlador PKCS n°11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	La ranura no contiene ninguna señal PKCS n°11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	El pin/contraseña para acceder a la señal PKCS n°11 no es válido.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se puede abrir el proveedor de servicios de cifrado basado en hardware. El nombre CSP no se ha especificado correctamente o se ha realizado un intento fallido de acceder al almacén de certificados CSP.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Conflicto de establecimiento de atributos entre PKCS11, base de datos de claves CMS y Microsoft Crypto API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	La función solicitada no recibe soporte en la plataforma en la que se ejecuta la aplicación. Por ejemplo, Microsoft Crypto API no se admite en plataformas que no sean Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Se ha devuelto un valor incorrecto desde la función de devolución de llamada del tipo restablecer sesión. Sólo se permite GSKit <code>gsk_sever_session</code> , <code>gsk_sever_session_with_cl_auth_0</code> o <code>gsk_sever_session_with_cl_auth_crit</code> .
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para <code>reset_cipher()</code> y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	No se ha especificado un ID válido para la llamada de la función <code>gsk_secure_soc_misc()</code> .
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID no válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificado.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de memoria caché SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido correctamente.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede reiniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de <code>gsk_start_trace()</code> debe ser un nombre completo de archivo de vía de acceso válido.

Tabla 2. Códigos de retorno de gestión de claves de IBM Global Security Kit

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Este mensaje lo emite cada llamada de función que se completa correctamente.
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función <code>open()</code> satisfactoria.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000005	5	GSK_INVALID_STATE	El manejador se encuentra en un estado incorrecto para la operación como, por ejemplo, ejecutar una operación init() en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar la criptografía.
0x0000000a	10	GSK_ERROR_ASN	Error al validar los campos ASN del certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves tiene un formato interno que no es válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlaces dinámicos de GSK. Asegúrese de que GSK se ha instalado correctamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Este mensaje indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido GSK_ENVIRONMENT_CLOSE_OPTIONS en GSK_DELAYED_ENVIRONMENT_CLOSE y se ha llamado a la función gsk_environment_close().

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el archivo stash por lo que no se ha inicializado el archivo de claves.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Una contraseña utilizada para una consulta LDAP no es correcta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato <code>gsk_secure_socket*()</code> después de una llamada a <code>gsk_close_environment()</code> .
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema se ha establecido en un valor que no es válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña especificada para el archivo de claves no es correcta. No se puede utilizar el archivo de claves. Es posible que el archivo de claves esté dañado.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.
0x0000019b	411	GSK_ERROR_BAD_MAC	El MAC no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	Se ha recibido del socio un protocolo SSL que no es válido.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	Error en read(). Informe de este error al servicio de soporte de software de IBM.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	Error en write(). Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El cifrado de la versión especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El cifrado de la versión 3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	No se ha creado el manejador. Informe de este error al servicio de soporte de software de IBM.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	La inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	El controlador PKCS n°11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	La ranura no contiene ninguna señal PKCS n°11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	El pin/contraseña para acceder a la señal PKCS n°11 es incorrecto.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se ha podido abrir el proveedor de servicios de cifrado basado en hardware (CSP). El nombre CSP no se ha especificado correctamente o se ha realizado un intento fallido de acceder al almacén de certificados CSP.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Se han definido algunos atributos conflictivos para la operación de SSL.
0x000001b4	436	GSK_CSP_OPEN_ERROR	La API de Microsoft Crypto sólo es compatible con Microsoft Windows 2000 con Service Pack 2 aplicado.
0x000001b5	437	GSK_CSP_OPEN_ERROR	El sistema se ejecuta en modalidad IPv6 sin establecer un PEERID.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para <code>reset_cipher()</code> y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Se ha especificado un ID que no es válido para la llamada de la función <code>gsk_secure_soc_misc()</code> .
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID que no es válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificado.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de memoria caché SID.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido correctamente.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede volver a iniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de <code>gsk_start_trace()</code> debe ser un nombre completo de archivo de vía de acceso válido.

Glosario

Este glosario proporciona términos y definiciones para IBM Spectrum Protect, IBM Spectrum Protect Snapshot y los productos asociados.

En este glosario se utilizan las referencias cruzadas siguientes:

- *Consulte* le remite de un término no preferido al término preferido o de una abreviatura a la forma completamente deletreada.
- *Consulte también* le refiere a un término contrastante relacionado.

Para otros términos y definiciones, consulte el sitio web Terminología de IBM®.

B C D E F G H I J K L M N O P Q R S T U V W

A

ACK

Consulte acuse de recibo.

ACL

Consulte lista de control de accesos.

activar

Para validar el contenido de un conjunto de políticas y convertirlo en conjunto de políticas activas.

acuse de recibo (ACK)

La transmisión de caracteres de reconocimiento como respuesta positiva a una transmisión de datos.

administrador

Una persona responsable de las tareas administrativas tales como la autorización de acceso y la gestión de contenidos. Los administradores también pueden otorgar niveles de autoridad a los usuarios.

Agente de almacenamiento

Programa que permite al cliente realizar operaciones de copia de seguridad y de restauración de datos del cliente directamente en y desde el almacenamiento conectado a una red de área de almacenamiento (SAN).

agregado

Objeto almacenado en una o varias agrupaciones de almacenamiento formado por un grupo de archivos lógicos empaquetados juntos. Consulte también archivo lógico, archivo físico.

agrupación de almacenamiento

Conjunto de volúmenes de almacenamiento o contenedores que es el destino utilizado para almacenar datos de cliente. Consulte también agrupación de datos activos, agrupación de almacenamiento de contenedores de nube, agrupación de almacenamiento de copias, agrupación de almacenamiento de contenedores de directorio, agrupación de almacenamiento primario, jerarquía de almacenamiento.

agrupación de almacenamiento de contenedores

Agrupación de almacenamiento primario que un servidor utiliza para almacenar datos. Los datos se almacenan en contenedores en directorios de sistema de archivos o en almacenamiento en la nube. Se eliminan los datos duplicados, si es necesario, mientras el servidor graba datos en la agrupación de almacenamiento. Consulte también agrupación de almacenamiento de contenedores de nube, contenedor, agrupación de almacenamiento de contenedores de directorio.

agrupación de almacenamiento de contenedores de directorio

Agrupación de almacenamiento que un servidor utiliza para almacenar datos en contenedores en los directorios de agrupación de almacenamiento. Los datos almacenados en una agrupación de almacenamiento de contenedores de directorio pueden utilizar la deduplicación de datos en línea o del lado del cliente. Consulte también agrupación de almacenamiento de contenedores de nube, agrupación de almacenamiento de contenedores, agrupación de almacenamiento de copia de contenedor, agrupación de almacenamiento.

agrupación de almacenamiento de contenedores de nube

Agrupación de almacenamiento que un servidor utiliza para almacenar datos en el almacenamiento en la nube. El almacenamiento en la nube puede estar ubicado en los locales o fuera de los locales. Consulte también agrupación de almacenamiento de contenedores, agrupación de almacenamiento de contenedores de directorio, agrupación de almacenamiento.

agrupación de almacenamiento de copia

Conjunto con nombre de volúmenes que contiene copias de archivos que residen en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copia se utilizan sólo para realizar copias de seguridad de los datos almacenados en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copia no pueden ser el destino de grupos de copia de seguridad o copias archivadas, ni de una clase de gestión (para archivos gestionados por espacio). Consulte también destino, grupo de almacenamiento principal, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

agrupación de almacenamiento de copia de contenedor

Agrupación de almacenamiento que un servidor utiliza para almacenar copias de extensiones de las agrupaciones de almacenamiento de contenedores de directorio. Estas copias se utilizan para reparar daños en una agrupación de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor utilizan soportes secuenciales como, por ejemplo, cinta. Consulte también agrupación de almacenamiento de contenedores de directorio.

agrupación de almacenamiento primaria

Conjunto de volúmenes o contenedores con nombre que el servidor utiliza para almacenar versiones de copia de seguridad de archivos, copias archivadas y archivos migrados desde nodos cliente. Consulte también grupo de almacenamiento de copias, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

agrupación de datos activos

Conjunto con nombre de volúmenes de agrupación de almacenamiento que contiene sólo versiones activas de datos de copia de seguridad de clientes. Consulte también almacenamiento del servidor, agrupación de almacenamiento, volumen de agrupación de almacenamiento.

aleatorización

Proceso de distribuir horas de inicio de planificaciones para diferentes cliente dentro de un porcentaje especificado en la ventana de inicio de planificación.

algoritmo Nagle

Algoritmo que reduce la congestión de las redes TCP/IP mediante la combinación de paquetes más pequeños y envío conjunto de los mismos.

almacenamiento del servidor

Las agrupaciones primarias, de copia y de almacenamiento de datos activos utilizados por el servidor para almacenar archivos de usuario como versiones de copia de seguridad, copias de archivo y archivos migrados desde nodos de clientes de gestión de almacenamiento jerárquico (archivos gestionados por espacio). Consulte también agrupación de datos activos, agrupación de almacenamiento de contenedores, agrupación de almacenamiento de copias, agrupación de almacenamiento primario, volumen de agrupación de almacenamiento, volumen.

almacén de datos

En un entorno virtualizado, la ubicación donde están almacenados los datos de máquina virtual.

ampliar

Aumentar la porción de espacio disponible que se puede utilizar para almacenar información sobre bases de datos o registros de recuperación.

anotación empresarial

Proceso de enviar eventos desde un servidor a un servidor de eventos designados. El servidor de eventos conduce los eventos a receptores designados, por ejemplo una salida de usuario. Consulte también evento.

anotaciones de errores

Conjunto de datos o archivo utilizados para registrar información de errores sobre un producto o sistema.

antigüedad del archivo

Con el fin de establecer prioridades para la migración, el número de días transcurridos desde el último acceso a un archivo.

archivado

Copiar programas, datos o archivos en otro medio de almacenamiento, normalmente para su almacenamiento a largo plazo o por seguridad. Consulte también recuperar.

archivo dañado

Archivo físico en el cual se han detectado errores de lectura.

archivo de caché

Instantánea de un volumen lógico creada por un Agente de instantáneas de volúmenes lógicos. Los bloques se guardan de forma inmediata antes de ser modificados durante la copia de seguridad de imagen y sus extensiones lógicas se guardan en los archivos de la caché.

archivo de caducidad

Archivo migrado o premigrado que está marcado para caducidad y eliminación del almacenamiento. Si se suprime del sistema de archivos local un archivo de resguardo o una copia original de un archivo premigrado, o bien si se actualiza la copia original de un archivo premigrado, el archivo migrado o premigrado correspondiente se marca para que caduque la siguiente vez que se ejecute una reconciliación.

archivo de configuración de dispositivo

1. En un servidor, un archivo que contiene información acerca de clases de dispositivos definidas y, en algunos servidores, bibliotecas y unidades definidas. La información es una copia de la información de configuración del dispositivo de la base de datos.
2. En un agente de almacenamiento, un archivo que contiene el nombre y contraseña de un agente de almacenamiento e información acerca del servidor que está gestionando las bibliotecas asociadas a SAN y las unidades que dicho agente de almacenamiento utiliza.

archivo de historial de volumen

Archivo que contiene información sobre volúmenes que han sido utilizados por el servidor para realizar copias de seguridad de bases de datos y para exportar datos del administrador, nodo, políticas o servidor. El archivo contiene también información acerca de volúmenes de agrupación de almacenamiento de acceso secuencial que se han agregado, reutilizado o suprimido. La información es una copia de la información del volumen grabada en la base de datos del servidor.

archivo de inclusión/exclusión

Archivo que contiene sentencias para determinar los archivos de los que se debe obtener copia de seguridad y las clases de gestión asociadas que se deberán utilizar a efectos de copia de seguridad o archivado. Consulte también lista de inclusión-exclusión.

archivo de macro

Archivo que contiene uno o varios comandos de administración de IBM Spectrum Protect, que se pueden ejecutar sólo desde un cliente administrativo mediante el comando MACRO. Consulte también el script del mandato IBM Spectrum Protect.

archivo de opciones

Archivo que contiene opciones de proceso. Consulte también archivo de opciones del sistema de clientes, archivo de opciones del usuario cliente.

archivo de opciones de cliente

Archivo editable que identifica al servidor y el método de comunicación y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación.

archivo de opciones del sistema cliente

Archivo, utilizado en clientes de sistemas AIX, UNIX, o Linux, que contiene un grupo de opciones de proceso que identifican los servidores con los que hay que ponerse en contacto para obtener servicios. Este archivo también especifica métodos de comunicación y opciones para la copia de seguridad, archivado, gestión jerárquica del almacenamiento y planificación. Consulte también usuario de clientes-archivos de opciones, archivo de opciones.

archivo de opciones del usuario cliente

Archivo que contiene el grupo de opciones de proceso utilizadas por los clientes del sistema. El grupo puede incluir opciones que determinan el servidor con el que el cliente se pone en contacto, y opciones que afectan a las operaciones de copia de seguridad, archivado, gestión de almacenamiento jerárquico y planificación. Este archivo se denomina también archivo dsm.opt. Para los sistemas AIX, UNIX o Linux, consulte también el archivo de opciones del sistema. Consulte también el archivo de opciones-sistema de clientes , archivo de opciones.

archivo de opciones de servidor

Archivo que contiene los valores que controlan diversas operaciones del servidor. Estos valores afectan por ejemplo a las comunicaciones, dispositivos y rendimiento.

archivo de resguardo

Archivo que sustituye el archivo original de un sistema de archivos local cuando el archivo se migra al almacenamiento. Un archivo de resguardo contiene la información necesaria para recuperar un archivo migrado de un almacenamiento de servidor. También tiene información adicional que se puede utilizar para evitar que tenga que recuperarse un archivo migrado. Consulte también archivo migrado, archivo residente.

archivo de resguardo huérfano

Archivo para el cual no se puede encontrar un archivo migrado en el servidor al cual está contactando el nodo cliente para los servicios de gestión de espacio. Un archivo de resguardo puede quedar huérfano cuando, por ejemplo, se modifica el archivo de opciones del sistema cliente para que contacte un servidor distinto del servidor al que se migró el archivo.

archivo de trabajo

Un archivo generado que contiene información de configuración de un trabajo de migración. El archivo está en formato XML y puede crearse y editarse en el cliente de gestión de almacenamiento jerárquico (HSM) en la interfaz gráfica de usuario del cliente de Windows. Consulte también trabajo de migración.

archivo esparcido

Archivo que se crea con una longitud mayor que los datos que contiene, con lo que se dejan espacios vacíos para agregar datos en un futuro.

archivo especial

En sistemas AIX, UNIX, o Linux, archivo que define dispositivos del sistema o archivos temporales creados por procesos. Existen tres tipos básicos de archivos especiales: FIFO (el primero en entrar es el primero en salir); de bloques y de caracteres.

archivo físico

Objeto almacenado en una o varias agrupaciones de almacenamiento formado por un archivo lógico individual o por un grupo de archivos lógicos empaquetados juntos como agregado. Consulte también agregado, archivo lógico, ocupación física.

archivo gestionado por espacio

Un archivo que se migra desde un nodo de cliente mediante el cliente de gestión de almacenamiento jerárquico (HSM). El cliente de HSM recupera el archivo del nodo de cliente bajo petición.

archivo lógico

Archivo almacenado en una o varias agrupaciones de almacenamiento del servidor, por sí solo o como parte de un agregado. Consulte también agregado, archivo físico, ocupación física.

archivo migrado

Un archivo que se ha copiado desde un sistema de archivos local a un almacenamiento. Para los clientes de HSM en los sistemas UNIX o Linux, el archivo se sustituye por un archivo de resguardo en el sistema de archivos local. En sistemas Windows, la creación del archivo de resguardo es opcional. Consulte también estado del archivo, archivo pre-migrado, archivo residente, archivo migrado.

archivo premigrado

Un archivo que se ha copiado al almacenamiento del servidor, pero que no se ha reemplazado con un archivo migrado en el sistema de archivo local. Una copia idéntica del archivo reside en el sistema de archivos local y en el almacenamiento del servidor. Los archivos premigrados se dan en sistemas de archivos UNIX y Linux a los que se ha agregado gestión de espacio. Consulte también estado de archivo, archivo migrado, archivo residente.

archivo residente

En un sistema Windows, un archivo completo en un sistema de archivos local que también podría ser un archivo migrado porque en el almacenamiento del servidor existe una copia migrada. En un sistema UNIX o Linux, un archivo completo en un sistema de archivos local que no ha sido migrado o pre-migrado o que ha sido recuperado del almacenamiento del servidor y modificado.

asociación

Relación definida entre un nodo cliente y una planificación de cliente. Las asociaciones identifican el nombre de la planificación, el nombre del dominio de políticas al que pertenece la planificación y el nombre del nodo de cliente que realiza operaciones planificadas.

asociación de perfil

En un gestor de configuración, relación definida entre un perfil y un objeto, como por ejemplo un dominio de políticas. Las asociaciones de perfil definen la información de configuración que se distribuye a un servidor gestionado cuando éste se suscribe al perfil.

atributo ampliado (EA)

Pares de valores o nombres que se asocian con archivos o directorios. Hay tres clases de atributos ampliados: de usuarios, del sistema y acreditados.

auditar

Buscar inconsistencias lógicas entre la información que tiene el servidor y la condición real del sistema. El gestor de almacenamiento puede auditar información sobre elementos como volúmenes, bibliotecas y licencias. Por ejemplo, cuando un gestor de almacenamiento audita un volumen, el servidor busca inconsistencias entre la información sobre archivos de los que se ha realizado una copia de seguridad o archivado almacenados en la base de datos y los datos reales asociados con cada versión de copia de seguridad o archivado en el almacenamiento del servidor.

AutoFS

consulte sistema de archivos montado automáticamente.

autorización

Derecho para acceder a objetos, recursos o funciones. Consulte también clase de privilegios.

B

base de datos de archivos premigrados

Base de datos que contiene información sobre cada archivo que ha sido pre-migrado al almacenamiento del servidor.

biblioteca

1. Un repositorio para medios grabados desmontables, como discos magnéticos o cintas magnéticas.
2. Una colección de una o más unidades, y posiblemente dispositivos robóticos (dependiendo del tipo de biblioteca), que se pueden usar para acceder a los volúmenes de almacenamiento.

biblioteca compartida

Dispositivo de biblioteca utilizado por diversos servidores de gestión de almacenamiento.

biblioteca de cintas

Conjunto de equipamiento y recursos que admiten un entorno de cintas de instalación. La biblioteca de cintas puede incluir bastidores de almacenamiento de cintas, mecanismos para el montaje de cintas automático, un conjunto de unidades de cinta y un conjunto de volúmenes de cinta relacionados montados en dichas unidades.

biblioteca externa

Una colección de unidades que es gestionada por el sistema de gestión de medios distinto al servidor de gestión de almacenamiento.

C

caché

Colocar una copia duplicada de un archivo en acceso aleatorio cuando el servidor migra un archivo a otra agrupación de almacenamiento de la jerarquía.

CAD

Consulte daemon de aceptación de clientes.

caducidad

Proceso en que los archivos, conjuntos de datos u objetos se identifican para su supresión debido a que se ha alcanzado su fecha de caducidad o ha transcurrido su periodo de retención.

capacidad estimada

Espacio disponible, en megabytes, en una agrupación de almacenamiento.

carácter comodín

Carácter especial como un asterisco (*) o una interrogación (?) que puede utilizarse para representar uno o varios caracteres. Cualquier carácter o juegos de caracteres puede sustituir al carácter comodín.

carácter de coincidencia de patrón

Consulte comodín.

centro de datos

En un entorno virtualizado, un contenedor que contiene hosts, clústeres, redes y almacenes de datos.

clase de dispositivo

Conjunto de características con nombre que se aplica a un grupo de dispositivos de almacenamiento. Cada clase de dispositivo tiene un nombre exclusivo y representa un tipo de dispositivo específico, como un disco, un disco óptico o una cinta.

clase de gestión

Objeto de política que los usuarios pueden vincular a cada archivo para especificar el modo en que el servidor debe gestionar el archivo. La clase de gestión puede contener un grupo de copias de seguridad, un grupo de copias de archivado y atributos de gestión del espacio. Consulte también enlazar, grupo de copias, cliente de gestión de almacenamiento jerárquico, conjunto de políticas, volver a enlazar.

clase de gestión predeterminada

Clase de gestión asignada a un juego de políticas. Esta clase se utiliza para controlar las copias de seguridad o copias archivadas cuando un archivo no está explícitamente asociado con una clase de gestión específica mediante la lista de inclusión/exclusión.

clase de privilegios

Nivel de autorización concedido a un administrador. La clase de privilegios determina que tareas de administración puede realizar el administrador. Consulte también autorización, clase de privilegios de nodo, clase de privilegios del operador, clase de privilegios de política, clase de privilegio de almacenamiento, clase de privilegio del sistema.

clase de privilegios de administración

Consulte clase de privilegios.

clase de privilegios de almacenamiento

Clase de privilegios que concede al administrador autorización para controlar el modo en que se asignan y utilizan los recursos de almacenamiento del servidor, por ejemplo supervisando la base de datos, el registro de recuperación y el almacenamiento del servidor. Consulte también clase de privilegios.

clase de privilegios del sistema

- Clase de privilegios que concede a un administrador autorización para emitir todos los comandos del servidor. Consulte también clase de privilegios.
- clase de privilegios de nodo
Clase de privilegios que concede a un administrador autorización para acceder de forma remota a clientes de copia de seguridad/archivado de un nodo de cliente específico o de todos los clientes de un dominio de políticas. Consulte también clase de privilegios.
- clase de privilegios de operador
Clase de privilegios que concede al administrador autorización para deshabilitar o detener el servidor, habilitar el mismo, cancelar procesos de éste y gestionar soportes de almacenamiento extraíbles. Consulte también clase de privilegios.
- clase de privilegios de política
Clase de privilegios que permite a un administrador gestionar objetos de políticas, inscribir nodos cliente y planificar operaciones de cliente para los nodos cliente. La autorización se puede limitar a determinados dominios de políticas. Consulte también clase de privilegios.
- Client Acceptor
Un servicio que sirve el applet Java™ para el cliente web a los navegadores web. En los sistemas Windows, la aceptación de clientes se instala y ejecuta como un servicio. En sistemas AIX, UNIX y Linux, la aceptación de clientes se ejecuta como un daemon.
- cliente
Programa de software u ordenador que solicita servicios desde un servidor. Consulte también servidor.
- cliente administrativo
Programa que se ejecuta en un servidor de archivos, una estación de trabajo o un sistema principal que los administradores utilizan para controlar y supervisar el servidor. Consulte también el cliente de archivo de copia de seguridad.
- cliente de aplicación
Programa instalado en un sistema para proteger una aplicación. El servidor proporciona servicios de copia de seguridad a un cliente de aplicaciones.
- cliente de biblioteca
Servidor que utiliza la comunicación servidor a servidor para acceder a una biblioteca gestionada por otro servidor de gestión de almacenamiento. Consulte también gestor de biblioteca.
- cliente de copia de seguridad y archivado
Programa que se ejecuta en un servidor de archivos o estación de trabajo y que facilita el medio para que los usuarios puedan efectuar operaciones de copia de seguridad, archivado, restauración y recuperación de archivos. Consulte también cliente administrativo.
- cliente de gestión de almacenamiento jerárquico (cliente HSM)
Programa de cliente que trabaja con el servidor para proporcionar la gestión de almacenamiento jerárquico (HSM) para un sistema. Consulte también gestión de almacenamiento jerárquico, clase de gestión.
- Cliente HSM
Consulte cliente de gestión de almacenamiento jerárquico.
- cliente/servidor
Pertenece al modelo de interacción de un proceso de datos distribuidos en el que un programa de un ordenador envía una solicitud a un programa de otro ordenador y espera una respuesta. El programa solicitante se denomina cliente; el programa que envía la respuesta se denomina servidor.
- Colección de juegos de copias de seguridad
Grupo de juegos de copias de seguridad creados a la vez y con el mismo nombre, descripción y clase de dispositivo. El servidor identifica cada juego de copias de seguridad de la colección mediante su nombre de nodo, nombre de juego y tipo de archivo.
- complemento
Un módulo de software que se puede instalar por separado y que añade funciones al programa aplicación o interfaz existente.
- compresión
Una función que elimina los caracteres repetitivos, espacios, series de caracteres o datos binario de los datos que se están procesando y reemplazan caracteres con caracteres de control. La compresión reduce la cantidad de espacio de almacenamiento que se requiere para los datos. Consulte también compresión en línea.
- compresión en línea
Un método para reducir espacio de almacenamiento. Los caracteres repetitivos, espacios, series de caracteres i datos binarios se eliminan según se van grabando datos en una agrupación de almacenamiento de contenedores. Consulte también compresión.
- configuración empresarial
Método de configuración de servidores de forma que el administrador pueda distribuir la configuración de uno de los servidores al resto utilizando la comunicación servidor a servidor. Consulte también gestor de configuración, servidor gestionado, perfil, suscripción.
- conjunto de nodos GPFS
Grupo montado y definido de sistemas de archivos GPFS.
- conjunto de opciones de cliente
Grupo de opciones definidas en el servidor y utilizadas en los nodos de cliente junto con archivos de opciones del cliente.
- contenedor

Ubicación de almacenamiento de datos, por ejemplo, un archivo, directorio o dispositivo. Consulte también agrupación de almacenamiento de contenedores.

convenio de nomenclatura universal (UNC)
El nombre de servidor y el nombre de la red combinados. Estos nombres identifican conjuntamente el recurso en el dominio.

conversación
Conexión entre dos programas en una sesión que les permite comunicarse durante el proceso o transacción.

copia archivada
Archivo o grupo de archivos de los que se ha realizado copias archivadas en el servidor de almacenamiento.

copia de duplicación
Instantánea de un volumen. La instantánea se puede realizar mientras las aplicaciones del sistema siguen grabando datos en los volúmenes.

copia de reserva
Copia de seguridad completa en la que no se suprimen los archivos de registro de transacciones para que los procedimientos de copia de seguridad que utilizan copias de seguridad incrementales o diferenciales no se vean afectados.

copia de seguridad activada
Copia de seguridad en la que el volumen está disponible para otras aplicaciones del sistema durante la operación.

copia de seguridad adaptable de subarchivos
Tipo de copia de seguridad que sólo envía las partes modificadas de un archivo al servidor en lugar de enviar todo el archivo. La copia de seguridad adaptable de subarchivos reduce el tráfico de la red e incrementa la velocidad de la operación de copia de seguridad.

copia de seguridad completa
Proceso de realizar una copia de seguridad de la base de datos de servidor completa. Cada copia de seguridad completa inicia una nueva serie de copia de seguridad de base de datos. Consulte también serie de copia de seguridad de la base de datos, instantánea de la base de datos, copia de seguridad en aumento.

copia de seguridad con registro por diario
Método de copia de seguridad para los clientes Windows y los clientes AIX que hacen uso del mecanismo de notificación de cambio de archivo para mejorar el rendimiento de la copia de seguridad incremental reduciendo la necesidad de explorar todo el sistema de archivos.

copia de seguridad de grupo
Copia de seguridad de un grupo que contiene una lista de archivos de uno o más orígenes de espacio de archivos.

copia de seguridad de imagen
Copia de seguridad de todo un sistema de archivos o de un volumen lógico RAW como un solo objeto.

copia de seguridad del volumen lógico
Copia de seguridad de un sistema de archivos o volumen lógico como un único objeto.

copia de seguridad de traspaso de datos de VSS
Operación de copia de seguridad que utiliza un proveedor de hardware del servicio de copia de volúmenes (VSS) de Microsoft (instalado en un sistema alternativo) para mover datos al servidor. Este tipo de copia de seguridad transfiere la carga de copia de seguridad de la máquina de producción a otra máquina.

copia de seguridad de volumen desactivado
Copia de seguridad en la que el volumen está bloqueado para que no puedan acceder al mismo otras aplicaciones del sistema durante la operación.

copia de seguridad difusa
Versión de copia de seguridad de un archivo que puede no reflejar fielmente el contenido actual del archivo, debido a que se realizó la copia de seguridad del mismo a la vez que se estaba modificando.

copia de seguridad incremental
Proceso de copia de seguridad de archivos o directorios o de copia de páginas en la base de datos, que son nuevas o se han cambiado desde la última copia de seguridad completa o incremental. Consulte también copia de seguridad selectiva.

copia de seguridad selectiva
Proceso de realizar copias de seguridad de determinados archivos o directorios de un dominio de cliente. Se realiza la copia de seguridad de los archivos que no se han excluido en la lista de inclusión-exclusión. Estos archivos deben cumplir los requisitos para la serialización en el grupo de copia de seguridad de la clase de gestión asignada a cada archivo. Consulte también copia de seguridad incremental.

Copia de seguridad VSS
Operación de copia de seguridad que utiliza la tecnología de servicio de copia de duplicación de volúmenes (VSS) de Microsoft. La operación de copia de seguridad produce una instantánea en línea (copia coherente de instante específico). Esta copia puede almacenarse en volúmenes de duplicación local o en el almacenamiento del servidor.

copia difusa
Versión de copia de seguridad o copia archivada de un archivo que puede no reflejar con total exactitud el contenido original del archivo, puesto que la copia de seguridad o archivado se ha realizado mientras el archivo se estaba modificando.

cuota

1. Para HSM en sistemas AIX, UNIX o Linux, el límite (en megabytes) sobre la cantidad de datos que se pueden migrar y los pre-migrados desde un sistema de archivos a un almacenamiento del servidor.
2. Para HSM en los sistemas Windows, un límite definido por el usuario al espacio que ocupan los archivos recuperados.

D

daemon

Programa que se ejecuta de forma desatendida para realizar funciones continuas o periódicas como el control de red.

daemon de aceptación de clientes (CAD)

Consulte aceptación de clientes.

daemon de registro por diario

En sistemas AIX, UNIX, o Linux, programa que realiza el seguimiento de las actividades de cambio en archivos que residen en sistemas de archivos.

daemon de supervisión de espacio

Daemon que comprueba la utilización del espacio de todos los sistemas de archivos para los que está activa la gestión de espacio y empieza automáticamente la migración por umbral cuando la utilización del espacio de un sistema de archivos iguala o supera su umbral superior.

datos iniciales

Bytes de datos iniciales de un archivo migrado que se almacenan en el archivo de resguardo correspondiente en el sistema de archivos local. La cantidad de datos iniciales que se almacenan en un archivo de resguardo depende del tamaño de apéndice especificado.

deduplicación de datos de postproceso

Método de reducción de necesidades de almacenamiento eliminando datos redundantes. Primero los datos se graban en la agrupación de almacenamiento, los datos duplicados se identifican y, a continuación, se reclama espacio en la agrupación de almacenamiento. Consulte también deduplicación de datos, deduplicación de datos en línea.

deduplicación de datos en línea

Método de reducción de necesidades de almacenamiento eliminando datos redundantes. Los datos se deduplican a medida que se graban en la agrupación de almacenamiento de contenedores. Consulte también deduplicación de datos, deduplicación de datos de postproceso.

destinatario

Repositorio del servidor que contiene un registro de mensajes del servidor y el cliente como eventos. Por ejemplo, un receptor puede ser una salida de archivo, una salida de usuarios o la consola del servidor y un registro de actividad. Consulte también evento.

destino

Atributo de grupo de copias o clase de gestión que especifica la agrupación de almacenamiento primaria en la que se realizará la copia de seguridad, archivado o migración del archivo cliente. Consulte también grupo de almacenamiento de copias.

detección automática

Característica que detecta, envía informes y actualiza el número de serie de una unidad o biblioteca de la base de datos cuando se define la ruta del servidor local.

dirección IP

Una dirección exclusiva para un dispositivo o una unidad lógica en una red que utiliza el estándar del protocolo de Internet.

dominio

Agrupación de nodos de cliente con uno o varios conjuntos de políticas que gestiona datos o recursos de almacenamiento para los nodos de cliente. Consulte también dominio de la política.

dominio de cliente

Conjunto de unidades, sistemas de archivos o volúmenes que un usuario selecciona para efectuar la operación de copia de seguridad o de archivado con el cliente de copia de seguridad/archivado.

dominio de políticas

Agrupación de usuarios de políticas con uno o varios conjuntos de políticas que gestiona datos o recursos de almacenamiento para los usuarios. Los usuarios son nodos de cliente asociados con el dominio de políticas. Consulte también conjunto de políticas activas, dominio.

DRM

Consulte gestor recuperación ante siniestro.

DSMAPI

Consulte interfaz de programación de aplicaciones de gestión de almacenamiento de datos.

duplicación

Proceso de grabar los mismos datos en varios discos al mismo tiempo. La duplicación de datos protege los datos de su pérdida en la base de datos o en el registro de recuperación.

E

EA

Consulte atributo ampliado.

EB

Consulte exabyte.

EFS

Consulte Sistema de archivos de cifrado.

eliminación de datos duplicados

Método de reducción de necesidades de almacenamiento eliminado datos redundantes. Sólo una instancia de los datos queda retenida en medios de almacenamiento. Otras instancias de los mismos datos son reemplazadas con un puntero a la instancia retenida. Consulte también deduplicación de datos en línea, deduplicación de datos de postproceso.

espacio de archivos

Espacio lógico de un almacenamiento de servidor que contiene un grupo de archivos de los que un nodo de cliente ha realizado una copia de seguridad o archivado desde una partición lógica individual, sistema de archivos o punto de montaje virtual. Los nodos de cliente pueden restaurar, recuperar o eliminar sus espacios de archivo del almacenamiento del servidor. En almacenamiento del servidor, los archivos pertenecientes a un espacio de archivos individual no se almacenan necesariamente juntos.

espacio de archivos activado para Unicode

Un espacio de archivos con un nombre que sigue el estándar de Unicode y es compatible con cualquier entorno local en estaciones de trabajo multilingües.

espacio de archivos estabilizado

Espacio de archivos que existe en el servidor pero no en el cliente.

espacio de archivos virtual

Representación de un directorio de un sistema de archivos NAS (almacenamiento conectado a red) como ruta a dicho directorio.

estación de trabajo

Un terminal o sistema personal en el que un usuario puede ejecutar aplicaciones y que a menudo está conectado a un sistema principal o red.

estado de archivo

Modalidad de gestión de espacio de un archivo que reside en un sistema de archivos al que se ha agregado la gestión de espacios. El estado de un archivo puede ser: residente, premigrado o migrado. Consulte también archivo migrado, archivo migrado previamente, archivo residente.

estado de sistema de archivos

Modalidad de gestión del almacenamiento de un sistema de archivos que reside en una estación de trabajo en que se ha instalado un cliente de gestión de almacenamiento jerárquica (HSM). El estado de un sistema de archivos puede ser: nativo, activo, inactivo o inactivo global.

estado inactivo global

Estado de todos los sistemas de archivos a los que se ha agregado gestión de espacio cuando ésta se desactiva globalmente para un nodo cliente.

evento

Aparición de importancia para una tarea o un sistema. Los sucesos pueden incluir la finalización o la anomalía de una operación, una acción de usuario, o el cambio de estado de un proceso. Consulte también anotación empresarial, receptor.

exabyte (EB)

Para el procesador, las capacidades de almacenamiento real y virtual y el volumen del canal, 2 a la potencia de 60 o 1 152 921 504 606 846 976 bytes. En la capacidad de almacenamiento de disco y el volumen de comunicaciones, 1 000 000 000 000 000 bytes.

excluir

Proceso de identificar archivos de una lista de inclusión-exclusión. Este proceso impide que se obtenga copia de seguridad de los archivos o se migren cuando un usuario o una planificación inicien una operación de copia incremental o selectiva. Un archivo puede excluirse de la copia de seguridad, de un gestor de espacio o de la copia de seguridad o del gestor de espacio.

extensión

Parte de un archivo que se crea durante el proceso de eliminación de duplicados de datos. Las extensiones se comparan con otras extensiones de archivo para identificar duplicados.

F

formato de datos no nativo

Formato de datos grabado en una agrupación de almacenamiento que difiere del formato utilizado por el servidor en las operaciones. Consulte también formato nativo.

formato nativo

Formato de datos que se escribe en un grupo de almacenamiento directamente mediante el servidor. Consulte también formato de datos no nativos.

frecuencia

Atributo de grupo de copia que especifica el intervalo mínimo, en días, que ha de transcurrir entre copias de seguridad incrementales.

FSID

Consulte ID de espacio de archivos.

FSM

Consulte migrador de sistema de archivos.

G

GB

Consulte **gigabyte**.

generación de contraseñas

Proceso que crea y almacena una nueva contraseña en un archivo de contraseñas cifrado cuando caduca la anterior. La generación automática de una contraseña evita que se solicite una contraseña.

General Parallel File System (GPFS)

Sistema de archivos de disco compartido de alto rendimiento que puede proporcionar acceso de datos desde nodos de un entorno de sistema en clúster. Consulte también **gestión del ciclo de vida de información**.

gestión de almacenamiento jerárquico (HSM)

Función que distribuye y gestiona automáticamente datos de un disco, cinta o ambos considerando los dispositivos de este tipo y potencialmente de otros como niveles de una jerarquía de almacenamiento que comprende desde dispositivos rápidos y caros a dispositivos más lentos, baratos y quizá extraíbles. Los objetivos son minimizar el tiempo de acceso a los datos y maximizar la capacidad de medios disponible. Consulte también **cliente de gestión de almacenamiento jerárquico**, **volver a llamar**, **jerarquía de almacenamiento**.

gestión de espacio

Consulte **gestión de almacenamiento jerárquico**.

gestión del ciclo de vida de la información (ILM)

Sistema de gestión de archivos basado en políticas para grupos de almacenamiento y conjuntos de archivos. Consulte también **General Parallel File System**.

gestor de biblioteca

Servidor que controla las operaciones de dispositivos cuando diversos servidores de gestión de almacenamiento comparten un dispositivo de almacenamiento. Consulte también **cliente de biblioteca**.

gestor de configuración

Servidor que distribuye información de configuración como políticas y planificaciones a servidores gestionados de acuerdo con sus perfiles. La información de configuración puede incluir políticas y planificaciones. Consulte también **configuración empresarial**, **servidor gestionado**, **perfil**.

gestor de recuperación de desastres (DRM)

Función que ofrece asistencia en la preparación y utilización de un archivo de plan de recuperación ante siniestro al servidor.

gigabyte (GB)

En el almacenamiento de procesador, almacenamiento real y almacenamiento virtual y el volumen de canal, dos elevado a la potencia de 30 o 1.073.741.824 bytes. Para capacidad de almacenamiento de disco y volumen de comunicaciones, 1.000.000.000 bytes.

GPFS

Consulte **General Parallel File System**.

grupo

Contenedor de almacenamiento en la nube utilizado por Amazon Simple Storage Service (Amazon S3).

grupo de copia

Objeto de políticas que contiene atributos que controlan cómo se generan las versiones de copias de seguridad o copias archivadas, el lugar donde deben ubicarse inicialmente y cuándo deben caducar. Un grupo de copias pertenece a una clase de gestión. Consulte también **grupo de copias archivadas**, **grupo de copias de seguridad**, **versión de copia de seguridad**, **clase de gestión**.

grupo de copias de archivado

Objeto de política que contiene atributos que controlan la generación, el destino y la caducidad de copias archivadas. Consulte también **copiar grupo**.

grupo de copias de seguridad

Objeto de política que contiene atributos que controlan la generación, destino y caducidad de archivos de copia de seguridad. Un grupo de copias pertenece a una clase de gestión. Consulte también **copiar grupo**.

grupo de políticas

Grupo de reglas de un dominio de políticas. Las reglas especifican la forma en que los datos o los recursos de almacenamiento se gestionan automáticamente en los nodos cliente de un dominio de políticas. Las reglas pueden aparecer en clases de gestión. Consulte también **conjunto de políticas activas**, **clase de gestión**.

grupo de políticas activas

Juego de políticas activado que contiene las reglas de políticas que utilizan actualmente todos los nodos cliente asignados al dominio de políticas. Consulte también **dominio de la política**, **conjunto de políticas**.

grupo de proximidad

Grupo de nodos cliente definido por el usuario cuyos datos se almacenan en un número mínimo de volúmenes a través del proceso de proximidad.

GUID

Consulte **identificador exclusivo global**.

H

hora de acceso a archivo

Para sistemas AIX, UNIX, o Linux, hora a la que se accedió por última vez al archivo.

HSM

Consulte gestión de almacenamiento jerárquico.

I

ID de espacio de archivos (FSID)

Identificador numérico único que el servidor asigna a un espacio de archivos cuando éste se guarda en el almacenamiento del servidor.

identificador exclusivo global (GUID)

Número determinado algorítmicamente que identifica de forma única una entidad de un sistema. Consulte también Identificador exclusivo universal.

identificador exclusivo universal (UUID)

Identificador numérico de 128 bits utilizado para garantizar que dos componentes no tengan el mismo identificador. Consulte también identificador exclusivo global.

ILM

Consulte gestión del ciclo de vida de la información.

imagen

Sistema de archivos o volumen lógico RAW del que se realiza una copia de seguridad en un objeto individual.

inodo

La estructura interna que describe los archivos individuales de sistemas AIX, UNIX, o Linux. Un inodo contiene el nodo, tipo, propietario y ubicación de un archivo.

inscripción abierta

Proceso de inscripción en el que los usuarios pueden inscribir en el servidor sus propias estaciones de trabajo como nodos cliente. Consulte también registro cerrado.

inscripción cerrada

Proceso de inscripción en que un administrador inscribe las estaciones de trabajo como nodos de cliente con el servidor. Consulte también registro abierto.

instantánea

Un tipo de instantánea que consiste en una vista de un instante específico de un volumen.

instantánea de base de datos

Copia de seguridad completa de toda la base de datos a un soporte que se pueda llevar a otro lugar. Cuando se crea una instantánea de base de datos, la serie de copia de seguridad de base de datos actual no se interrumpe. Las instantáneas de bases de datos no pueden tener copias de seguridad de bases de datos incrementales asociadas. Consulte también serie de copia de seguridad de la base de datos, copia de seguridad completa.

interfaz de programación de aplicaciones de gestión de almacenamiento de datos (DSMAPI)

Conjunto de funciones y semántica que supervisa eventos en archivos y gestiona y mantiene los datos de un archivo. En un entorno de HSM, una DSMAPI utiliza los eventos para notificar a las aplicaciones de gestión de datos acerca de las operaciones realizadas en los archivos, almacena información de atributos arbitraria de un archivo, admite regiones gestionadas de un archivo y utiliza los derechos de acceso de DSMAPI para controlar el acceso a un objeto de archivo.

intervalo de inicio

Periodo de tiempo durante el que debe iniciarse una planificación.

J

jerarquía de almacenamiento

Orden lógico de las agrupaciones de almacenamiento primario, definido por el administrador. Normalmente, el orden se basa en la velocidad y capacidad de los dispositivos utilizados por las agrupaciones de almacenamiento. La jerarquía de almacenamiento se define identificando la siguiente agrupación de almacenamiento en una definición de agrupaciones de almacenamiento. Consulte también agrupación de almacenamiento.

juego de copias de seguridad

Un grupo consolidado y portable de versiones activas de archivos de copia de seguridad que se generan para un cliente de copia de seguridad/archivado.

K

KB

Consulte kilobyte.

kilobyte (KB)

En almacenamiento de procesador, almacenamiento real y virtual y volumen de canal, 2 elevado a la décima potencia, o 1.024 bytes. Para capacidad de almacenamiento de disco y volumen de comunicaciones, 1.000 bytes.

L

LAN

Consulte red de área local.

límite de montajes

Número máximo de volúmenes a los que se puede acceder simultáneamente desde la misma clase de dispositivo. El límite de montajes determina el número máximo de puntos de montaje. Consulte también punto de montaje.

lista de control de accesos (ACL)

En la seguridad del sistema, lista asociada a un objeto que identifica todos los temas que pueden acceder al objeto y a sus derechos de acceso.

lista de exclusión/inclusión

Consulte lista de inclusión/exclusión.

lista de inclusión/exclusión

Lista de opciones que incluye o excluye los archivos seleccionados para la copia de seguridad. Una opción excluye identifica los archivos de los que no se debe realizar copia. Una opción de inclusión identifica los archivos que están exentos de las reglas de exclusión o asigna una clase de gestión a un archivo o grupo de archivos, para los servicios de copia de seguridad o archivado. Consulte también incluir-excluir archivo.

local

1. Perteneciente a un dispositivo, archivo o sistema al que se accede directamente desde un sistema de usuario, sin utilizar una línea de comunicación.
2. Para los productos de gestión de almacenamiento jerárquico, relacionados con el destino de archivos migrados que se están moviendo. Consulte también remoto.

LOFS

Consulte sistema de archivos virtuales loopback.

Logical Volume Snapshot Agent (LVSA)

Software que puede actuar como el proveedor de instantáneas para crear una instantánea de un volumen lógico durante una copia de seguridad de imagen en línea.

LUN

Consulte número de unidad lógica.

LVSA

Consulte Agente de instantáneas de volúmenes lógicos.

M

MB

Consulte megabyte.

megabyte (MB)

En el almacenamiento de procesador, el almacenamiento real y el volumen de canal, 2 a la potencia de 20 o 1.048.576 bytes. En capacidad de almacenamiento de disco y volúmenes de comunicaciones, 1.000.000 bytes.

metadatos

Datos que describen las características de los datos; datos descriptivos.

método de comunicación

Método mediante el cual intercambian información un cliente y un servidor. Consulte también Transmission Control Protocol/Internet Protocol.

migración

El proceso de mover datos de un sistema de computadora a otro, o una aplicación a otro sistema de computadora.

migración a petición

Proceso que se utiliza para responder a una situación de falta de espacio en un sistema de archivos en el que está activa la gestión de almacenamiento jerárquico (HSM). Los archivos se migran al almacenamiento del servidor hasta que el porcentaje de utilización de espacio alcanza el umbral inferior que se ha establecido para el sistema de archivos. Si los umbrales superior e inferior son iguales, se migra un archivo. Consulte también migración automática, migración selectiva, migración de umbral.

migración automática

Proceso utilizado para traspasar automáticamente archivos desde un sistema de archivos local al almacenamiento, basándose en las opciones y valores que ha escogido un usuario root en la estación de trabajo. Consulte también migración de demandas, migración de umbral.

migración por umbral

Capacidad inferior y superior de las agrupaciones de almacenamiento o sistemas de archivos, expresada en porcentajes, en las que debe iniciarse y detenerse la migración.

migración por umbral

El proceso de mover archivos de un sistema de archivos local a un almacenamiento de servidor basado en los umbrales bajo y alto que se definen para el sistema de archivos. Consulte también migración automática, migración de demanda, trabajo de migración, migración selectiva.

migración selectiva

Proceso de copiar archivos seleccionados por el usuario desde un sistema de archivos local a un almacenamiento del servidor y reemplazar los nuevos archivos con archivos de resguardo en el sistema de archivos local. Consulte también migración de demandas, migración de umbral.

migrador de sistema de archivos (FSM)

Extensión de kernel que intercepta todas las operaciones de sistema de archivos y proporciona la gestión de espacio necesaria. Si no se requiere soporte de gestión del espacio, la operación se envía al sistema operativo, que realiza sus funciones normales. El migrador del sistema de archivos se monta sobre un sistema de archivos al agregar gestión de espacio al sistema de archivos.

migrar

Para mover los datos a otra ubicación o una aplicación a otro sistema de computadora.

modalidad

Atributo de grupo de copia que especifica si se debe realizar la copia de seguridad de un archivo que no se ha modificado desde la última copia de seguridad que se realizó. Consulte también modalidad absoluta, modalidad modificada.

modalidad Absoluta

En gestión de almacenamiento, modalidad de grupo de copia de seguridad que indica que un archivo o directorio se tendrán en cuenta para realizar la copia de seguridad incremental aunque el archivo o directorio no se hayan modificado desde la última operación de copia de seguridad. Consulte también modalidad, modalidad modificada.

modalidad de acceso

Atributo de una agrupación o volumen de almacenamiento que especifica si el servidor puede escribir o leer la agrupación o volumen de almacenamiento.

modalidad de planificación

Tipo de operación de planificación para el nodo del servidor y cliente que admite dos modalidades de planificación: sondeo de clientes y por petición de servidor.

modalidad de planificación de sondeo de clientes

Método de operación en el que el cliente solicita trabajo al servidor. Consulte también modalidad de planificación de indicación del servidor.

modalidad de planificación por petición de servidor

Técnica de comunicaciones entre el cliente y el servidor donde el servidor se pone en contacto con el nodo cliente cuando se tienen que realizar tareas. Consulte también modalidad de planificación de sondeo de clientes.

modalidad de recuperación de archivo parcial

Modalidad de recuperación que hace que la función de gestión de almacenamiento jerárquico (HSM) lea sólo una porción de un archivo migrado del almacenamiento, según lo requiera la aplicación que accede al archivo.

modalidad Modificados

En gestión de almacenamiento, modalidad de grupo de copia de seguridad que indica que un archivo o directorio se tendrá en cuenta para realizar la copia de seguridad incremental aunque el archivo no se haya modificado desde la última operación de copia de seguridad. Un archivo o directorio se considera modificado si ha cambiado la fecha, el tamaño, el propietario o los permisos. Consulte también modalidad absoluta, modalidad.

MTU

Consulte unidad de transmisión máxima.

N

named pipe

Tipo de comunicación entre procesos que permite que las corrientes de datos de los mensajes pasen entre los procesos de igual a igual, como sucede entre un cliente y un servidor.

NDMP

Consulte Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)

Interfaz estándar de redes y ordenadores personales que se utiliza en redes de área local para proporcionar mensajes y funciones de servidor de impresión y servidor de archivos. Los programas de aplicación que utilizan NetBIOS no tienen que manejar los detalles de protocolos LAN Data link control (DLC).

Network Basic Input/Output System

Consulte NetBIOS.

Network Data Management Protocol (NDMP)

Protocolo que permite a una aplicación de gestión de almacenamiento de red controlar las operaciones de copia de seguridad y recuperación de un servidor de archivos NDMP, sin instalar software del proveedor en ese servidor de archivos.

nodo

Servidor de archivos o estación de trabajo donde está instalado el programa cliente de copia de seguridad/archivado, que se ha registrado en el servidor.

Nodo agente

Nodo cliente al que se ha otorgado autorización proxy para realizar operaciones en nombre de otro nodo cliente, que es el nodo de destino.

nodo cliente

Servidor de archivos o estación de trabajo donde está instalado el programa cliente de copia de seguridad/archivado, que se ha registrado en el servidor.

nodo de destino

Nodo cliente para el que otros nodos cliente (denominados nodos agente) han recibido autorización de proxy. La autorización de proxy permite a los nodos cliente realizar operaciones de copia de seguridad y de restauración en nombre del nodo de destino,

que es propietario de los datos.

nodo del servidor de archivo NAS
Consulte el nodo NAS.

nodo NAS
Un nodo de cliente es un servidor de archivos de almacenamiento conectado a red (NAS). Los datos de los nodos NAS se transfieren mediante un servidor de archivos NAS controlado por el Network data management protocol (NDMP). Los nodos NAS reciben también el nombre de nodo de servidor de archivos NAS.

nombre de ámbito mundial (WWN)
Identificador de nombre sin firma de 64 bits exclusivo.

nombre del nodo
Nombre exclusivo que se utiliza para identificar una estación de trabajo, servidor de archivos o PC en el servidor.

número de inodo
Número que especifica un archivo de inodo particular del sistema de archivos.

número de unidad lógica (LUN)
En el estándar SCSI (interfaz para pequeños sistemas), se utiliza un identificador exclusivo para diferenciar dispositivos, cada uno de los cuales es una unidad lógica (LU).

O

objeto de marca de archivo borrado
Pequeño subconjunto de atributos de un objeto suprimido. El objeto de marca de archivo borrado se retiene durante un periodo específico, y al final de ese periodo específico, se suprime de forma permanente.

objeto gestionado
Definición de la base de datos del servidor gestionado que un gestor de configuración ha distribuido al servidor gestionado. Cuando un servidor gestionado se suscribe a un perfil, todos los objetos asociados con dicho perfil pasan a ser objetos gestionados en la base de datos del servidor gestionado.

ocupación física
Cantidad de espacio utilizado por archivos físicos en una agrupación de almacenamiento. Este espacio incluye el espacio sin utilizar que se crea cuando se suprimen archivos lógicos de agregados. Consulte también archivo lógico, ocupación lógica, archivo físico.

ocupación lógica
Espacio utilizado por archivos lógicos en una agrupación de almacenamiento. Este espacio no incluye el espacio sin utilizar creado al suprimir archivos lógicos de archivos agregados, por lo que puede ser inferior a la ocupación física. Consulte también ocupación física.

optimización de almacenamiento
Consulte deduplicación de datos.

P

página
Unidad de espacio definida de un soporte de almacenamiento o volumen de base de datos.

paquete
En la comunicación de datos, secuencia de dígitos binarios, incluidos los datos y las señales de control, que se transmite y conmuta como un todo compuesto.

partición de carga de trabajo (WPAR)
Partición en una única instancia del sistema operativo.

perfil
Grupo de información de configuración con nombre que se puede distribuir desde un gestor de configuración a suscribir un servidor gestionado. La información de configuración puede incluir diversos ID de administrador registrados, políticas, planificaciones de clientes, juegos de opciones de clientes, planificaciones administrativas, scripts de comandos de gestores de almacenamiento, definiciones de servidores y definiciones de grupos de servidores. Consulte también gestor de configuración, configuración empresarial, servidor gestionado.

periodo de espera de montaje
Número máximo de minutos que el servidor espera por una solicitud de montaje de un volumen de acceso secuencial antes de cancelar la solicitud.

período de gracia de retención de copia de seguridad
Número de días que el gestor de almacenamiento conserva una versión de copia de seguridad cuando el servidor no puede volver a vincular el archivo a una clase de gestión apropiada.

período de gracia de retención de copias archivadas
Número de días que el gestor de almacenamiento retiene una copia archivada cuando el servidor no puede volver a vincular el archivo a una clase de gestión apropiada. Consulte también vincular.

periodo de retención de montaje
Número máximo de minutos que el servidor retiene un volumen de medio de acceso secuencial montado que no está en uso antes de desmontarlo.

plan de recuperación ante siniestro

Archivo que se crea mediante el gestor de recuperación de desastres (DRM) que contiene información sobre cómo recuperar sistemas de computadora si ocurre un desastre y scripts que se pueden ejecutar para realizar algunas tareas de recuperación. El archivo incluye información sobre el software y hardware utilizado por el servidor y la ubicación del soporte de recuperación.

planificación

Registro de base de datos que describe las operaciones del cliente o comandos de administración que se van a procesar. Consulte también planificación de comandos de administración, planificación de clientes.

planificación de cliente

Registro de base de datos que describe el proceso planificado de una operación del cliente durante un periodo de tiempo específico. La operación del cliente puede ser una copia de seguridad, archivado, restauración, recuperación, un comando de sistema operativo del cliente o una macro. Consulte también planificación de mandatos administrativos, planificador central, planificación.

planificación de comandos de administración

Registro de base de datos que describe el proceso planificado de un comando administrativo durante un periodo de tiempo específico. Consulte también programador central, programa central, programa.

planificador central

Función que permite a un administrador planificar operaciones de cliente y comandos de administración. Las operaciones pueden planificarse para que tengan lugar de forma periódica o en una fecha específica. Consulte también planificación de comandos de administración, planificación de clientes.

porcentaje de premigración

Valor establecido para la gestión de espacio que controla si los siguientes candidatos elegibles de un sistema de archivos se premigran durante la migración por umbral o la migración a petición.

prefijo de volumen de cinta

Cualificador de alto nivel del nombre de archivo o el nombre del conjunto de datos de la etiqueta de la cinta estándar.

pre migración

Proceso de copia de archivos que son elegibles para migración al almacenamiento del servidor, pero dejando el archivo original intacto en el sistema de archivos local.

protocolo de comunicación

Conjunto de interfaces definidas que permite a los sistemas comunicarse entre sí.

proximidad

Proceso mediante el que se mantienen todos los datos que pertenecen a un único espacio de archivos de cliente, a un único nodo cliente o a un grupo de nodos cliente en un número mínimo de volúmenes de acceso secuencial de una agrupación de almacenamiento. La proximidad puede reducir el número de volúmenes a los que se debe acceder cuando es necesario restaurar un gran volumen de datos.

punto de montaje

Unidad lógica por la que se accede a los volúmenes en una clase de dispositivo de acceso secuencial. En tipos de dispositivos de medios extraíbles, como una cinta, un punto de montaje es una unidad lógica asociada a una unidad física. En el tipo de dispositivo de archivos, un punto de montaje es una unidad lógica asociada con una corriente de E/S. Consulte también límite de montajes.

punto de montaje virtual

Una ramificación de un directorio de un sistema de archivos que se define como el sistema de archivos virtuales. El sistema de archivos virtuales crea una copia de seguridad en su propio espacio de archivos en el servidor. El servidor procesa el punto de montaje virtual como un sistema de archivos por separado, pero el sistema operativo del cliente no lo hace así.

punto de validación

Un punto en el tiempo cuando los datos se consideran coherentes.

Q

R

reclamación

Proceso de consolidar los datos restantes de muchos volúmenes de acceso secuencial en menos volúmenes de acceso secuencial.

reconciliación

Proceso para asegurar la coherencia entre el repositorio de datos original y el sistema de mayor tamaño donde se almacenan los datos para la copia de seguridad. Los servidores de almacenamiento u otros sistemas de almacenamiento son ejemplos de sistemas de mayor tamaño donde se almacenan los datos para la copia de seguridad. Durante el proceso de reconciliación, se eliminan los datos que se han identificado como ya no necesarios.

recuperación

Para copiar un archivo migrado desde un almacenamiento del servidor de vuelta a su sistema de archivos de origen usando el cliente de gestión de almacenamiento jerárquico. Consulte también recuperación selectiva.

recuperación selectiva

Proceso de copiar los archivos seleccionados por el usuario desde un almacenamiento del servidor a un sistema de archivos local. Consulte también recuperación, recuperación transparente.

recuperación transparente

El proceso que se utiliza para recuperar automáticamente un archivo migrado a una estación de trabajo o servidor de archivos cuando se accede al archivo. Consulte también recuperación selectiva.

recuperar

Copiar información archivada de la agrupación de almacenamiento en la estación de trabajo para su uso. La operación de recuperación no afecta a la versión archivada en la agrupación de almacenamiento. Consulte también archivar.

red de área de almacenamiento (SAN)

Red de almacenamiento dedicada adaptada a un entorno específico, que combina servidores, sistemas, productos de almacenamiento, productos de red, software y servicios.

red de área local (LAN)

Red que conecta diversos dispositivos en un área limitada (un edificio o campus, por ejemplo) y que se puede conectar a una red mayor.

registrar

Definir un nodo cliente o ID de administrador que pueda acceder al servidor.

registro

Repositorio que contiene información de acceso y configuración sobre usuarios, sistemas y software.

registro de actividades

Registro que registra los mensajes de actividad normal generados por el servidor. Estos mensajes contienen información relativa a las operaciones del servidor y de los clientes, como por ejemplo, la hora de inicio de las sesiones o errores de E/S de dispositivos.

registro de eventos

Registro de base de datos que describe el estado actual y los resultados de eventos.

registro de recuperación

Registro de actualizaciones que están a punto de grabarse en las bases de datos. Se puede utilizar este registro para realizar recuperaciones tras errores del sistema y de los soportes. El registro de recuperación está compuesto por el registro activo (incluyendo el duplicado del registro) y los registros de archivado.

regla de autenticación

Especificación que permite a otro usuario restaurar o recuperar archivos del almacenamiento.

remoto

Para los productos de gestión de almacenamiento jerárquico, relacionados con el origen de archivos migrados que se están moviendo. Consulte también local.

rendimiento

En gestión de almacenamiento, los bytes totales de la carga de trabajo, excluyendo la sobrecarga, de los que se realiza la copia de seguridad o restauración, divididos por el tiempo transcurrido.

resguardo

Acceso directo en el sistema de archivos Windows generado por el cliente de gestión de almacenamiento jerárquico (HSM) para un archivo migrado que permite el acceso transparente por parte de los usuarios. Un resguardo es la representación como archivo disperso de un archivo migrado, con un punto de reanálisis adjunto.

restauración

Copiar información desde la ubicación de la copia de seguridad a la ubicación del almacenamiento activo para su uso. Por ejemplo, copiar información del almacenamiento del servidor a una estación de trabajo del cliente.

restauración de buzón

Función que restaura datos de Microsoft Exchange Server (de copias de seguridad de IBM Data Protection for Microsoft Exchange) a nivel del buzón o elemento de buzón.

restauración de buzón individual

Consulte restauración de buzón.

Restauración instantánea VSS

Operación que restaura datos de una instantánea local. La instantánea de la copia de seguridad de VSS que reside en un volumen de duplicación local. La operación de restauración recupera los datos al utilizar un método de restauración asistido por medio de hardware (por ejemplo, una operación de FlashCopy).

Restauración rápida VSS

Operación que restaura datos de una instantánea local. La instantánea de la copia de seguridad de VSS que reside en un volumen de duplicación local. La operación de restauración recupera los datos utilizando un método de copia a nivel de archivo.

Restauración VSS Restauraciones VSS restauraciones VSS

Función que utiliza un proveedor de software del servicio de copia de volúmenes (VSS) de Microsoft para restaurar instantáneas que residen en el almacenamiento del servidor. Las instancias las crearon una copia de seguridad de VSS y se almacenan en su ubicación original.

retención

El espacio de tiempo, en días, que se conservarán en la agrupación de almacenamiento las copias de seguridad o copias archivadas inactivas antes de ser eliminadas. Los atributos de grupo de copia y los periodos de gracia predeterminados de retención correspondientes al dominio definen la retención.

revincular

Asociar todas las versiones de copia de seguridad de un archivo con un nuevo nombre de clase de gestión. Por ejemplo, un archivo que tiene una versión de copia de seguridad activa se revincula cuando se realiza una copia de seguridad de una versión

posterior del archivo file con una asociación de clase de gestión distinta. Consulte también enlazar, clase de gestión.

rol de autorización

Especificación que permite a otro usuario restaurar o recuperar los archivos de un usuario del almacenamiento.

ruta

Objeto que define una relación uno a uno entre una fuente y un destino. A través de la ruta, la fuente accede al destino. Los datos se puede mover de la fuente al destino y viceversa. Un ejemplo de fuente es un transportador de datos (por ejemplo un servidor de archivos de almacenamiento conectado a red (NAS)), y un ejemplo de destino es una unidad de cintas.

S

SAN

Consulte red de área de almacenamiento.

script

Serie de comandos, combinados en un archivo, que desempeñan una función determinada cuando se ejecuta el archivo. Los scripts se interpretan cuando se ejecutan. Consulte también el script del mandato IBM Spectrum Protect.

Script de comandos de IBM Spectrum Protect

Secuencia de comandos de administración de IBM Spectrum Protect que se restauran en la base de datos del servidor de IBM Spectrum Protect. El script se puede ejecutar desde cualquier interfaz del servidor. El script puede incluir la sustitución de parámetros de comandos y lógica condicional. Consulte también el script del archivo de macro.

sección

Grupo de líneas de un archivo que, conjuntamente, tienen una función común o definen una parte del sistema. Las stanzas se suelen separar mediante líneas en blanco o caracteres de dos puntos, y cada una tiene un nombre.

Secure Sockets Layer (SSL)

Protocolo de seguridad que proporciona privacidad de comunicación. Con SSL, las aplicaciones cliente/servidor se pueden comunicar de una forma diseñada para evitar escuchas, sabotajes y falsificación de mensajes.

serialización

Proceso de manipular archivos modificados durante el proceso de copia de seguridad o archivado. Consulte también serialización dinámica compartida, serialización estática compartida, serialización estática.

serialización dinámica

Serialización de copias en la cual a un archivo o carpeta se le realiza una copia de seguridad o se archiva en el primer intento sin importar si cambia durante la copia de seguridad o archivado. Consulte también serialización dinámica compartida, serialización estática compartida, serialización estática.

serialización dinámica compartida

Valor para la serialización que especifica de qué archivo no debe realizarse copia de seguridad o archivado si éste está siendo modificado durante la operación. El cliente del archivo de copia de seguridad vuelve a intentar realizar la copia de seguridad o la operación de archivado varias veces; si el archivo está siendo modificado durante cada intento, el cliente del archivo de copia de seguridad realizará la copia de seguridad o archivará el archivo en su último intento. Consulte también serialización dinámica, serialización, serialización estática compartida, serialización estática.

serialización estática

Valor de serialización de grupo de copia que especifica que no se debe modificar un archivo durante una operación de copia de seguridad o archivado. Si el archivo está en uso durante el primer intento, el cliente de archivo de copia de seguridad no puede realizar la copia de seguridad ni archivar el archivo. Consulte también serialización dinámica, serialización, serialización dinámica compartida, serialización estática compartida.

serialización estática compartida

Valor de serialización de grupo de copia que especifica que no se debe modificar un archivo durante una operación de copia de seguridad o archivado. El cliente intenta volver a probar la operación varias veces. Si el archivo está siendo utilizado durante los reintentos, no se llevará a cabo la operación de copia de seguridad o archivado. Consulte también serialización dinámica, serialización, serialización dinámica compartida, serialización estática.

serie de copia de seguridad de base de datos

Copia de seguridad completa de la base de datos, más un máximo de 32 copias de seguridad incrementales realizadas tras dicha copia de seguridad completa. Cada copia de seguridad completa que se ejecuta inicia una nueva serie de copia de seguridad de base de datos. Cada serie se identifica con un número. Consulte también la instantánea de la base de datos, copia de seguridad completa.

servicio de diario

En Microsoft Windows, programa que realiza el seguimiento de las actividades de cambio de archivos que residen en sistemas de archivos.

Servicio de duplicación de volúmenes (VSS)

Conjunto de interfaces de programas de aplicación (API) de Microsoft que se utilizan para crear copias de seguridad de duplicación de volúmenes, copias exactas de archivos, incluidos todos los archivos abiertos, etc.

servidor

Programa de software o sistema que proporciona servicios a otros programas de software o sistemas. Consulte también cliente.

servidor de archivos

Sistema dedicado y sus dispositivos de almacenamiento periféricos conectados a una red de área local que almacena tanto programas como archivos compartidos por los usuarios en la red.

servidor de archivos de almacenamiento conectados a la red (servidor de archivos NAS)
Dispositivo de almacenamiento dedicado con un sistema operativo optimizado para funciones de servicio de archivos. Los servidores de archivos NAS pueden tener las características de un nodo y un transportador de datos.

servidor de archivos NAS
Consulte también servidor.

servidor de eventos
Servidor al que otros servidores pueden enviar eventos para su registro. El servidor de eventos conduce los eventos a todos los receptores designados habilitados para el envío de eventos.

servidor de medios
En un entorno de z/OS, programa que proporciona acceso al disco de z/OS y almacenamiento de cintas para servidores de IBM Spectrum Protect que se ejecutan en sistemas operativos distintos a z/OS.

servidor gestionado
Un servidor que recibe información de configuración de un gestor de configuración usando una suscripción a uno o más perfiles. La información de configuración puede incluir definiciones de objetos como políticas y planificaciones. Consulte también el gestor de configuración, configuración empresarial, perfil, suscripción.

servidor gestor de datos
Servidor que recoge información de metadatos para el inventario de cliente y gestiona transacciones para el agente de almacenamiento a través de la red de área local. El servidor gestor de datos informa al agente de almacenamiento con atributos de biblioteca aplicables y el identificador de volumen de destino.

sesión
Conexión lógica o virtual entre dos estaciones, programas de software o dispositivos de una red que permite que los dos elementos se comuniquen e intercambien datos durante la sesión. Consulte también sesión.

sesión administrativa
Periodo de tiempo durante el cual un identificador de usuario administrados se comunica con un servidor para realizar tareas administrativas. Consulte también sesión de nodo de cliente, sesión.

sesión de nodo cliente
Sesión en la que un nodo de cliente se comunica con un servidor para realizar solicitudes de copia de seguridad, restauración, archivado, migración o recuperación. Consulte también sesión.

sistema de archivos activo
Sistema de archivos al que se ha agregado la gestión de espacio. En la gestión de espacio, las tareas para sistemas de archivos activos incluyen la migración automática, la reconciliación, la migración selectiva y la recuperación. Consulte también el sistema de archivos inactivos.

Sistema de archivos de cifrado (EFS)
Sistema de archivos con cifrado de nivel de sistema de archivos.

sistema de archivos de origen
Sistema de archivos desde el que se ha migrado un archivo. Cuando se recupera un archivo, este se devuelve a su sistema de archivos de origen.

sistema de archivos inactivo
Sistema de archivos del que se ha desactivado la gestión de espacio. Consulte también sistema de archivo activo.

sistema de archivos montado automáticamente (AutoFS)
Sistema de archivos gestionado por un daemon de montaje automático. El daemon de montaje automático supervisa una ruta de directorio especificada y monta automáticamente el sistema de archivos para acceder a los datos.

sistema de archivos nativo
Sistema de archivos localmente agregado al servidor de archivos y no agregado para la gestión del espacio. El cliente del gestor de almacenamiento jerárquico (HSM) no ofrece servicios de gestión del espacio al sistema de archivos.

sistema de archivos virtuales loopback (LOFS)
Sistema de archivos que se crea montando un directorio sobre otro directorio local, también conocido como montaje sobre montaje. Un LOFS también puede generarse utilizando un montador automático.

sitio de recuperación
Consulte sitio secundario.

sitio primario
Un sitio virtual físico compuesto por los recursos de almacenamiento, red y hardware. Normalmente, las operaciones de producción se ejecutan en el sitio primario. Los datos se pueden duplicar en un sitio secundario para las operaciones de recuperación tras desastre y de migración tras error. Consulte también sitio secundario.

sitio protegido
Consulte sitio primario.

sitio secundario
Un sitio virtual o físico compuesto por recursos de almacenamiento, red y hardware que admiten las necesidades de recuperación del sitio primario. Cuando se produce una anomalía en el sitio primario, las operaciones pueden continuar en el sitio secundario. Consulte también sitio primario.

SSL
Consulte capa de sockets seguros.

suscripción

En un entorno de almacenamiento, el proceso de identificar los suscriptores a los cuales se distribuyen los perfiles. Consulte también configuración empresarial, servidor gestionado.

T

tamaño de archivo de resguardo

El tamaño de un archivo que reemplaza al archivo original en un sistema de archivo local cuando se migra el archivo a un almacenamiento de servidor. El tamaño que se especifica para los archivos de resguardo determina cuántos datos iniciales pueden almacenarse en éste. El valor predeterminado del tamaño de archivo de resguardo es el tamaño de bloque que se define para un sistema de archivos menos 1 byte.

TCA

Consulte trusted communications agent.

TCP/IP

Consulte Protocolo de control de transmisión/Protocolo de Internet.

tiempo de espera excedido

Intervalo de tiempo asignado a un evento para producirse o completarse antes de que se interrumpa la operación.

tipo de dispositivo de archivo

Tipo de dispositivo que especifica el uso de archivos de acceso secuencial en almacenamiento de disco como volúmenes.

trabajo de migración

Especificación de los archivos que se deben migrar y de las acciones que se deben realiza en los archivos originales tras la migración. Consulte también archivo de trabajo, migración de umbral.

transferencia de datos fuera de la LAN

Consulte traspaso de datos sin LAN.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Conjunto estándar sin marca de protocolos de comunicación que proporcionan conexiones fin a fin fiables entre aplicaciones en redes interconectadas de diferentes tipos. Consulte también el método de comunicación.

transportador de datos

Dispositivo que transporta datos en nombre del servidor. Un servidor de archivos de almacenamiento conectado a red (NAS) es un transportador de datos.

traspaso de datos fuera de la LAN

Traspaso de datos del cliente, desde el sistema cliente a un dispositivo de almacenamiento a través de una red de área de almacenamiento (SAN), pasando por alto la red de área local.

trusted communications agent (TCA)

Programa que manipula el protocolo de contraseña de inicio de sesión cuando los clientes utilizan la generación de contraseñas.

U

UCS-2

Esquema de codificado de 2 bytes (16 bits) basado en la especificación ISO/IEC 10646-1. UCS-2 define tres niveles de implementación: Nivel 1: no se permite ninguna combinación de elementos codificados; Nivel 2: sólo se permite la combinación de elementos codificados para tailandés, hindú, hebreo y árabe; Nivel 3: se permite cualquier combinación de elementos codificados.

umbral de reclamación

Porcentaje de espacio que un volumen de medio de acceso secuencial debe tener antes de que el servidor pueda reclamar el volumen. El espacio se puede reclamar cuando se caducan o se suprimen archivos.

UNC

Consulte convenio de nomenclatura universal.

Unicode

Un estándar de codificación de caracteres que permite el intercambio, el proceso y la visualización de texto que se graba en los lenguajes comunes de todo el mundo, además de muchos textos clásicos e históricos.

unidad máxima de transmisión (MTU)

El bloque más grande posible que puede enviarse en un medio físico determinado de una trama individual. Por ejemplo, la unidad de transmisión máxima para Ethernet es 1.500 bytes.

usuario autorizado

Un usuario tiene autorización administrativa para un cliente en una estación de trabajo. Este usuario puede cambiar contraseñas, realizar inscripciones abiertas y suprimir espacios de archivos.

usuario root

Usuario del sistema que opera sin limitaciones. Los usuarios root tienen los derechos y privilegios especiales necesarios para realizar tareas de administración.

UTF-8

Formato de codificación Unicode Transformation Format de 8 bites, diseñado de cara a la facilidad de uso con los sistemas existentes basados en ASCII. El valor CCSID para datos en formato UTF-8 es 1208.

utilización de recursos durante la sesión

Cantidad de tiempo de espera, tiempo del procesador y espacio utilizados y recuperados durante una sesión del cliente.

UUID

Consulte identificador exclusivo universal.

V

validar

Verificar un conjunto de políticas en busca de condiciones que pueden causar problemas si dicho conjunto pasa a ser el conjunto de políticas activo. Por ejemplo, el proceso de validación comprueba si el juego de políticas contiene una clase de gestión predeterminada.

velocidad de transferencia de datos compuesta

Estadística de rendimiento que indica el número medio de bytes transferidos por segundo durante el proceso de una operación determinada.

velocidad de transferencia de datos en red

Velocidad calculada dividiendo el número total de bytes transferidos por el tiempo de transferencia de los datos. Por ejemplo, esta velocidad puede ser el tiempo que se tarda en transferir datos en una red.

versión

Copia de seguridad de un archivo almacenada en un almacenamiento del servidor. La copia de seguridad más reciente de un archivo es la versión activa. Las copias anteriores de ese mismo archivo son versiones inactivas. El número de versiones conservadas por el servidor es determinado por los atributos del grupo de copia de la clase de gestión.

versión activa

La copia de seguridad más reciente de un archivo que ha almacenado. La versión activa de un archivo no puede suprimirse hasta que el proceso de copia de seguridad detecta que el usuario ha sustituido el archivo por una versión más nueva o que el archivo se ha suprimido del servidor de archivos o de la estación de trabajo. Consulte también la versión de copia de seguridad, versión inactiva.

versión de copia de seguridad

Un archivo o directorio al cual se creó una copia de seguridad del nodo de cliente para almacenamiento. En el almacenamiento del servidor puede haber más de una versión de copia de seguridad, aunque únicamente una de ellas es la versión activa. Consulte también versión activa, grupo de copias, versión inactiva.

versión inactiva

Versión de copia de seguridad de un archivo que no es la más reciente o corresponde a un archivo que ya no existe en el sistema cliente. Las versiones de copia de seguridad inactivas caducan dependiendo de la clase de gestión asignada al archivo. Consulte también versión activa, versión de copia de seguridad.

vincular

Asociar un archivo a un nombre de clase de gestión. Consulte también archivar-período de gracia de retención, clase de gestión, volver a enlazar.

volumen

Unidad discreta de almacenamiento en disco, cinta y otro soporte de grabación de datos que admite algún tipo de identificador y lista de parámetros, como una etiqueta de volumen o control de entrada/salida. Consulte también volumen reutilizable, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

volumen de agrupación de almacenamiento

Volumen que ha sido asignado a una agrupación de almacenamiento. Consulte también grupo de datos activos, grupo de almacenamiento de copias, grupo de almacenamiento primario, almacenamiento del servidor, volumen.

volumen de duplicación

Los datos almacenados de una instantánea de un volumen. La instantánea se puede realizar mientras las aplicaciones del sistema siguen grabando datos en los volúmenes.

volumen de duplicación local

Datos que se almacenan en volúmenes de duplicación que se encuentran en un subsistema de almacenamiento de disco.

volumen lógico

Una porción de un volumen físico que contiene un sistema de archivos.

volumen lógico RAW

Porción de un volumen físico que consta de bloques no asignados y no tiene definición JFS (journalled file system). Un volumen lógico RAW es accesible para lectura/escritura sólo a través de las funciones de E/S de bajo nivel.

volumen reutilizable

Volumen etiquetado en blanco o que contiene datos inválidos, que no está definido y que está disponible para el uso. Consulte también volumen.

volumen virtual

Archivo de archivado de un servidor de destino que representa un volumen de medios virtual de un servidor de origen.

VSS

Consulte servicio de copia de duplicación de volúmenes.

W

WPAR

Consulte partición de carga de trabajo.

WWN

Consulte nombre de ámbito mundial.